Wi-Fi Router X4 N300

WLR-4100

User Manual

Table of Contents

Introduction 3
Key Features 4
Package Contents 5
Cautions 6
Product Layout 7
Network + System Requirements 9
Setup your Router 10
Setup your Computer 11
Login to your Router 14
Configure your Internet connection 15
Configure your Router 18
Wireless Settings 23
Firewall Settings 31
Advanced Settings 35
Toolbox Settings 41
Addendum A: GNU/GPL Leaflet 48
Addendum A: USB Port Control Center 50
Addendum C: GNU/GPL 61
Addendum C: Declaration of Conformity 69

Revision 2.0

© Sitecom Europe BV 2013

Note: All the information contained in this manual was correct at the time of publication.

However, as our engineers are always updating and improving the product, your device's software may have a slightly different appearance or modified functionality than presented in this manual.

Introduction

Congratulations on your purchase of the WiFi Router X4 N300. This router is compliant with 802.11n and up to 6 times faster than standard 802.11g based routers while still being compatible with 802.11g & 802.11b devices. This router is not only a Wireless Access Point, but also doubles as a 4-port full-duplex Gigabit switch that connects your wired-Ethernet devices together at 10/100/1000 Mbps speeds.

At 300 Mbps wireless transmission rate, the Access Point built into the router uses advanced MIMO (Multi-Input, Multi-Output) technology to transmit multiple streams of data in a single wireless channel, giving you seamless access to multimedia content. The robust RF signal travels farther, eliminates dead spots and extends the network range. For data protection and privacy, the router encodes all wireless transmissions with WEP, WPA, or WPA2 encryption.

With the built-in DHCP Server & powerful SPI firewall, the router protects your computers against intruders and most known Internet attacks and also provides safe VPN pass-through. With the incredible speed and QoS function of 802.11n, the router is ideal for media-centric applications like streaming video, gaming, and VoIP telephony to run multiple media-intense data streams through the network at the same time, with no degradation in performance.

With Sitecom Cloud Security, Sitecom goes one step further and ensures that you can surf the Internet even more safely, not only on your PC, but on all the devices in your home which you use to access the Internet. It does not matter whether you surf the Internet on a laptop, a tablet, a mobile telephone or your television. Thanks to the security that is integrated in the router, all the Internet devices in your home are protected against the dangers of Internet criminality.

Key Features

Features	Advantages
Incredible Data Rate up to 300Mbps*	Heavy data payloads such as MPEG video streaming
IEEE 802.11n Compliant and backwards compatible with 802.11b/g	Fully Interoperable with IEEE 802.11b / IEEE802.11g compliant devices with legacy protection
Four 10/100/1000 Mbps gigabit Switch Ports (Auto-Crossover)	Scalability, extend your network.
Firewall supports Virtual Server Mapping, DMZ, IP Filter, ICMP Blocking, SPI	Avoids the attacks of Hackers or Viruses from Internet
Support 802.1x authenticator, 802.11i (WPA/WPA2, AES), VPN pass-through	Provide mutual authentication (Client and dynamic encryption keys to enhance security
Sitecom Cloud Security	Protect your home against cybercrime while browsing.
Guest Network (Firmware 2.0 and higher only)	Devices connected to the Guest network will have Internet connection but no access to the main network and cannot communicate with each other.
IPv6 support (Firmware 2.0 and higher only)	Support for Static, Native, 6RD and DS-Lite.

* Theoretical wireless signal rate based on IEEE standard of 802.11a, b, g, n chipset used. Actual throughput may vary. Network conditions and environmental factors lower actual throughput rate. All specifications are subject to change without notice.

Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped back in its original package.

- The WLR-4100 WiFi Router X4 N300
- A 110V~240V to 12V 1A Switching Power Adapter
- A Quick Install Guide
- An UTP cable

Cautions

This router's design and manufacturer has your safety in mind. In order to safely and effectively use this router, please read the following before usage.

Usage Cautions

The user should not modify this router. The environmental temperature should be within +5 ~ +35 degrees Celsius.

Power

The router's power voltage is DC 12V 1A.

When using this router, please connect the supplied AC adapter or AC adapter cable to the router's power jack. When placing the adapter cable, make sure it can't get damaged or be subject to pressure. To reduce the risk of electric shock, unplug the adapter first before cleaning it. Never connect the adapter to the router in a humid or dusty area. Do not replace the adapter or cable's wire or connector.

Repair

If the router has a problem, you should take it to an appointed repair center and let the specialists do the repair. Never repair the router yourself, you might damage the router or endanger yourself.

Disposing of the Router

When you dispose of the router, be sure to dispose it appropriately. Some countries may regulate disposal of an electrical device, please consult with your local authority.

Others

When using this router, please do not let it come into contact with water or other liquids. If water is accidentally spilled on the router, please use a dry cloth to absorb the spillage. Electronic products are vulnerable, when using please avoid shaking or hitting the router, and do not press the buttons too hard.

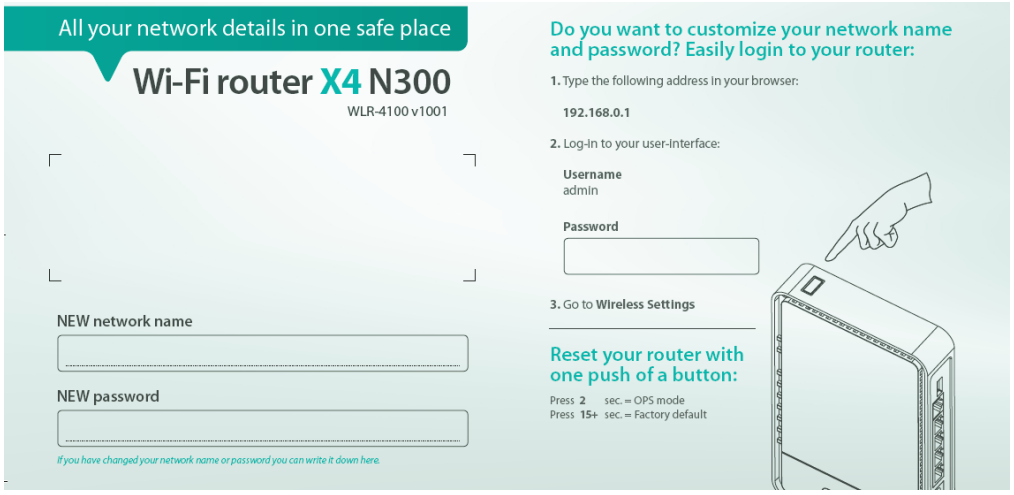
- Do not let the router come into contact with water or other liquid.
- Do not disassemble, repair or change the design of the router; any damage done will not be included in the repair policy.
- Avoid hitting the router with a hard object, avoid shaking the router and stay away from magnetic fields.
- If during electrostatic discharge or a strong electromagnetic field the product will malfunction, unplug the power cable. The product will return to normal performance the next time it is powered on.

Product Layout

Port	Description
Power connector	Connect the 12V DC adapter to this port
LAN (Yellow)	Connect your PCs or network devices to these ports
WAN (Blue)	Connect your ADSL/Cable modem to this port

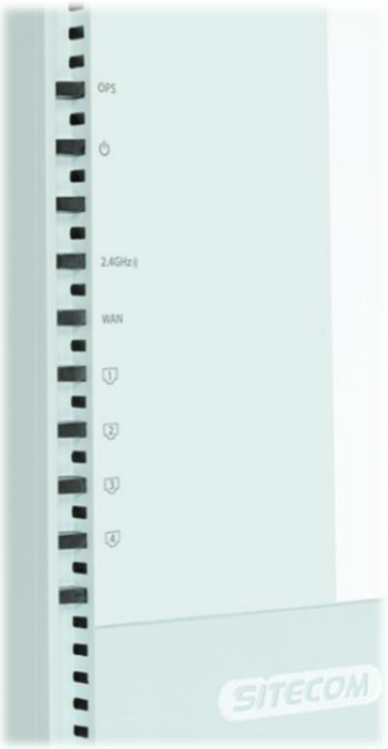
Backlabel and Network Details Folder

The Network Details Folder describes the IP address, login details, network name, security code and OPS button functionality.


All your network details in one safe place
Wi-Fi router X4 N300
WLR-4100 v1001
NEW network name
NEW password
If you have changed your network name or password you can write it down here.
Do you want to customize your network name and password? Easily login to your router:
1. Type the following address in your browser:
192.168.0.1
2. Log-in to your user-interface:
Username
admin
Password
3. Go to Wireless Settings
Reset your router with one push of a button:
Press 2 sec. = OPS mode
Press 15+ sec. = Factory default

Button	Description
OPS BUTTON	Press 0-5 seconds for OPS mode
	Press 15 Seconds to reset the router to factory defaults.

LED Definition



As shown from the top to the bottom.

Port	Description
OPS (White)	Shows OPS activity.
Power (Red)	Shows the device is turned on.
2.4GHz (Blue)	Shows 2.4GHz WiFi activity.
WAN (Blue)	Shows the WAN cable is connected.
LAN (Blue)	Shows the cable is connected.
LAN (Blue)	Shows the cable is connected.
LAN (Blue)	Shows the cable is connected.
LAN (Blue)	Shows the cable is connected.

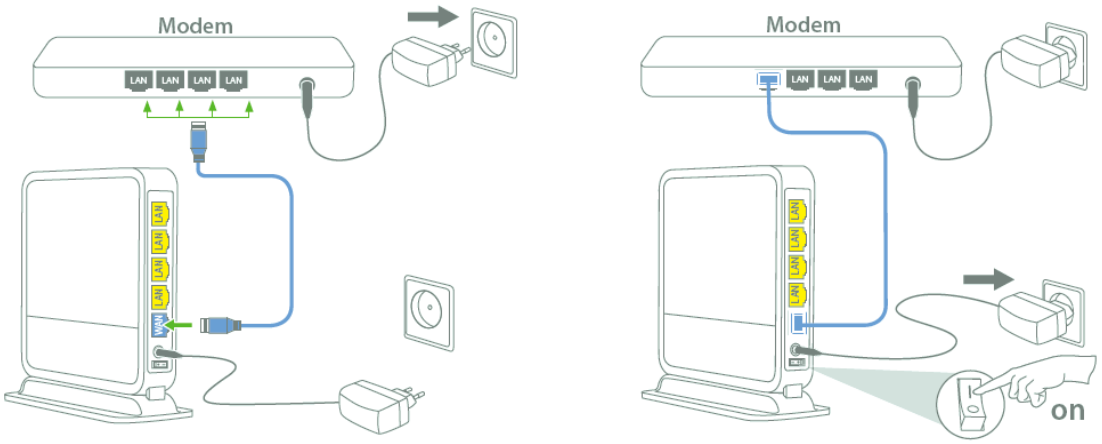
Network + System Requirements

To begin using the router, make sure you meet the following as minimum requirements:

- PC/Notebook.
- Operating System – Microsoft Windows XP/VISTA/7 or Mac OSX
- 1 Free Ethernet port.
- WiFi card/USB dongle (802.11 a/b/g/n) – optional.
- External xDSL (ADSL) or Cable modem with an Ethernet port (RJ-45).
- PC with a Web-Browser (Internet Explorer, Safari, Firefox, Opera)
- Ethernet compatible CAT5e cables.

Setup your Router

You can place the router on a desk or other flat surface, or you can mount it on a wall. For optimal performance, place your router in the center of your home (or your office) in a location that is away from any potential source of interference, such as a metal wall or microwave oven. This location must be close to a power connection and your ADSL/Cable modem.

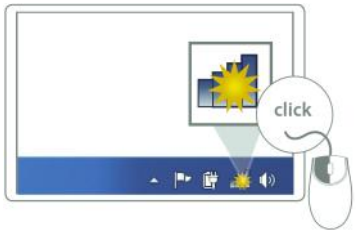


Connect the supplied power-adapter to the power inlet port and connect it to a wall outlet. Switch the router on by flipping the switch on the back of the device. The router automatically enters the self-test phase. During self-test phase, the Power LED will be lit continuously to indicate that this product is in normal operation.

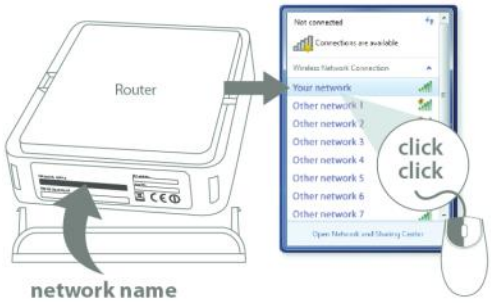
Setup your Computer

Windows, Manual Connection

- Click on the icon for wireless connectivity. This is usually located in the System Tray, next to the clock.

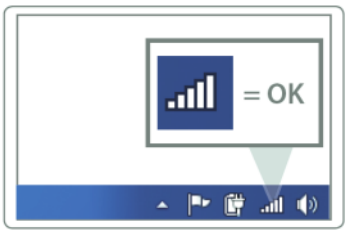


- Select the Sitecom network. The correct network name can be found on the sticker on bottom of the router, or in the Network Details Folder.



- Fill in the password for the wireless network. The correct password can be found on the sticker on the bottom of the router, or in the Network Details Folder.

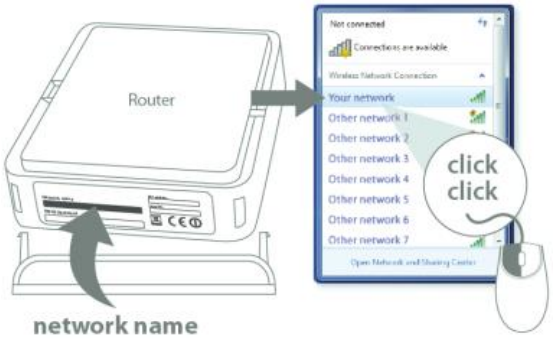
- Wait for the icon to display that it’s connected to the network.



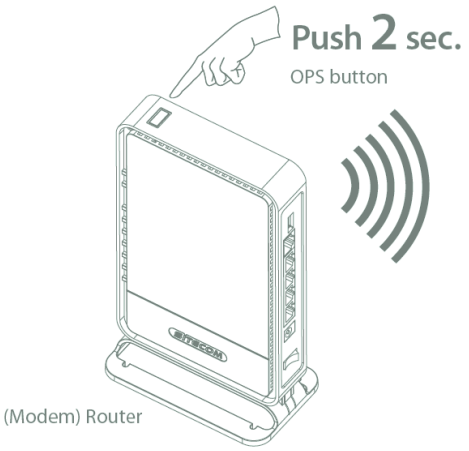
Windows, OPS Connection

- Click on the icon for wireless connectivity. This is usually located in the System Tray, next to the clock.

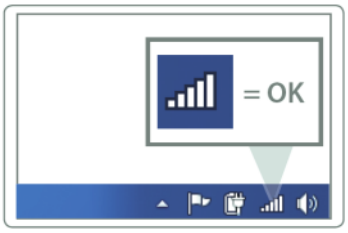
- Select the Sitecom network. The correct network name can be found on the sticker on bottom of the router, or in the Network Details Folder.



- Push the OPS Button on the router. Keep the button pushed for 0-5 seconds.



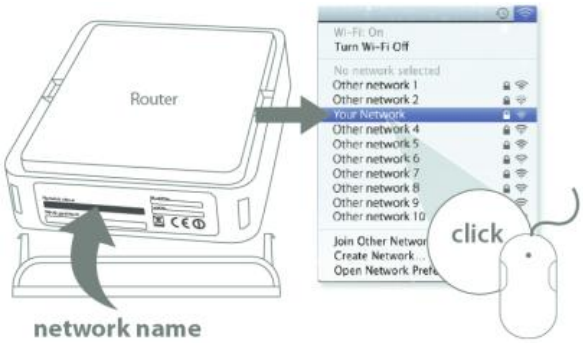
- Wait for the icon to display that it's connected to the network.



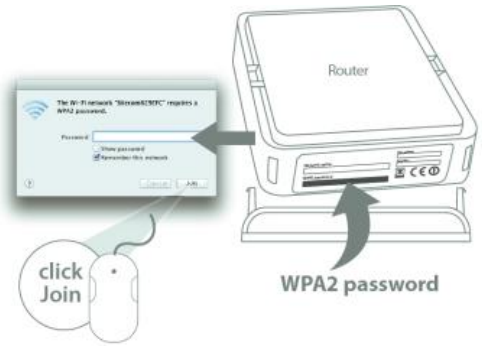
Mac OSX

- Click on the icon for wireless connectivity. This is usually located in the System Tray, next to the clock.

- Select the Sitecom network. The correct network name can be found on the sticker on bottom of the router, or in the Network Details Folder.



- Fill in the password for the wireless network. The correct password can be found on the sticker on the bottom of the router, or in the Network Details Folder.



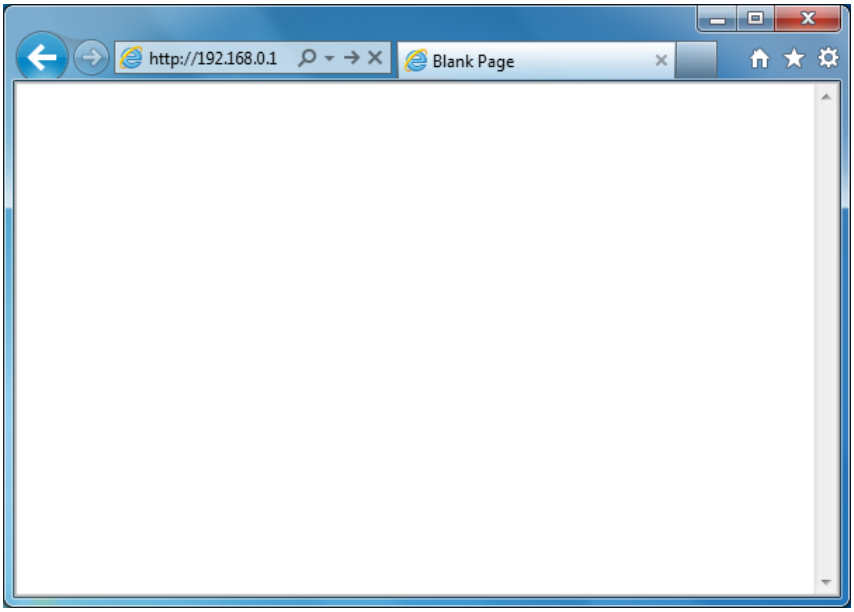
- Wait for the icon to display that it’s connected to the network.

Login to your Router

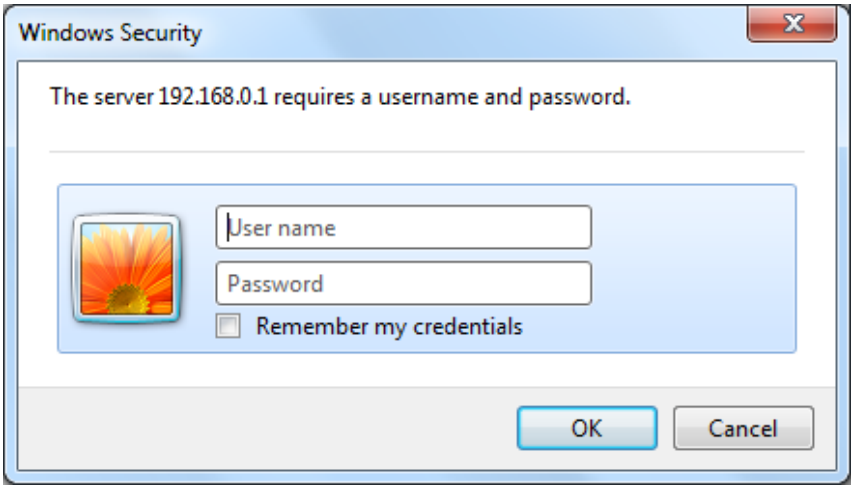
LOGIN procedure

- OPEN your browser (e.g. Internet Explorer).

- Type http://192.168.0.1 in the address bar and press [Enter]. For routers with Firmware 2.0 or higher you can also type http://sitecom.router.



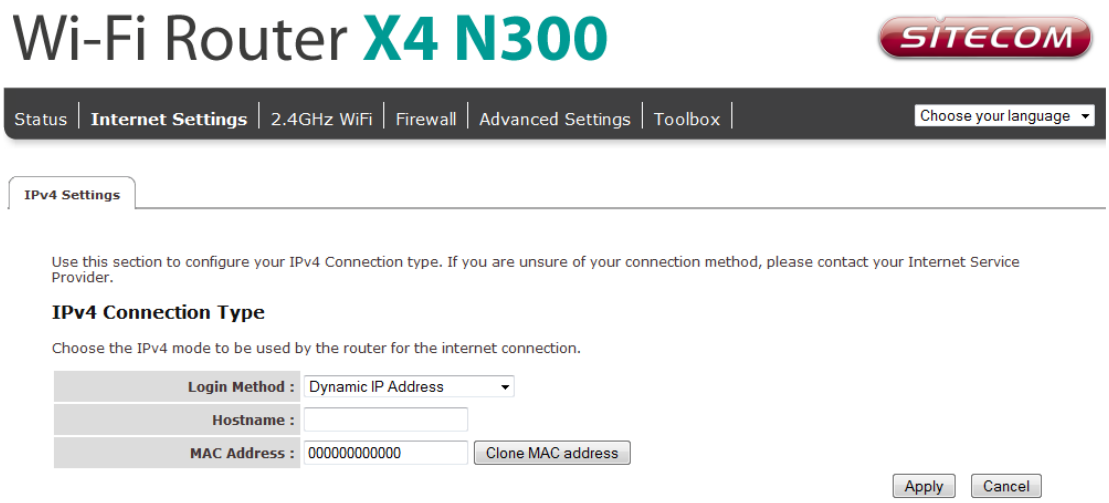
- Type user name and password. The default username is admin, the password can be found on the back label on the bottom of your router.



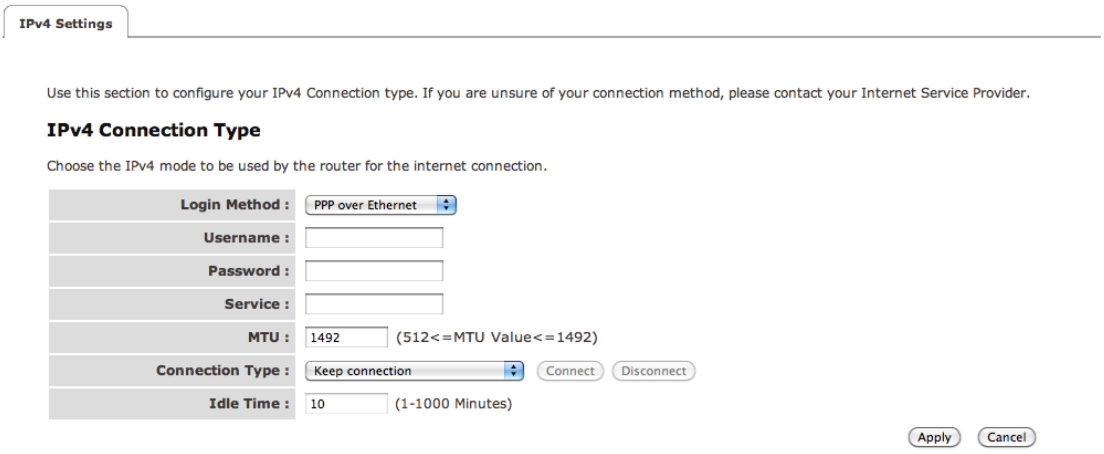
- Click OK.
- You will see the home page of the WiFi Router X4 N300.

Configure your Internet connection

From the menu, select “Internet Settings”.



Depending on the chosen setting, you may need to enter your user name and password, MAC address or hostname in the following window. After you have entered the correct information, click **Apply**.



IPv6 Configuration (Firmware 2.0 and up only)

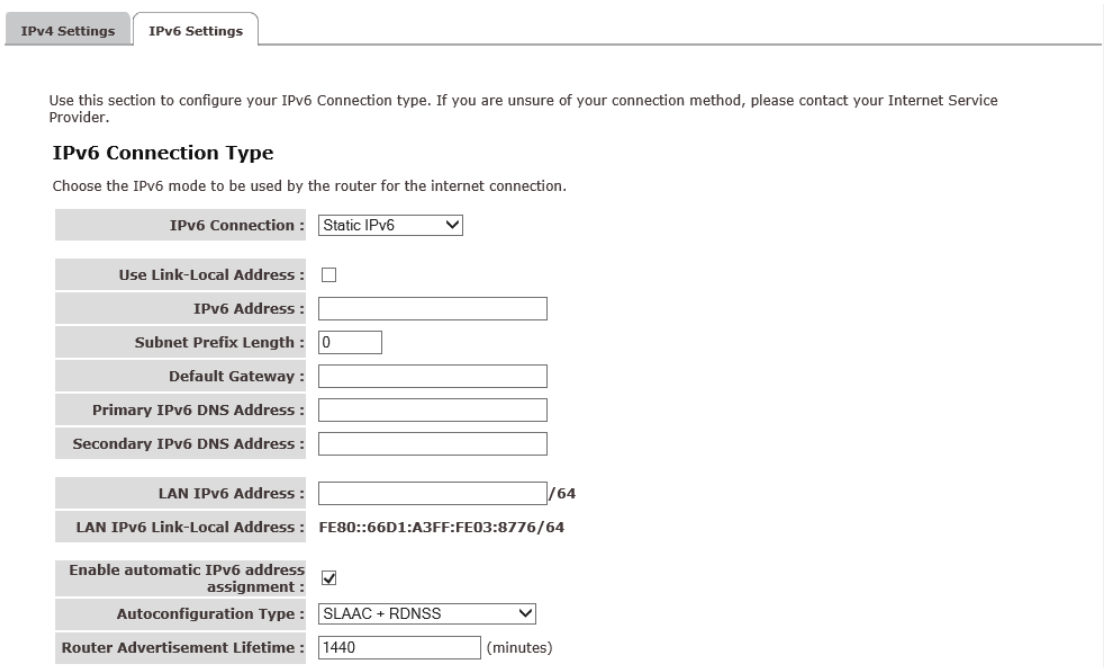
The IPv6 (Internet Protocol version 6) section is where you configure your IPv6 Connection type.

IPv6 Connection Type

There are several connection types to choose from: Static IPv6, Autoconfiguration, 6RD and Link-local only. If you are unsure of your connection method, please contact your IPv6 Internet Service Provider.

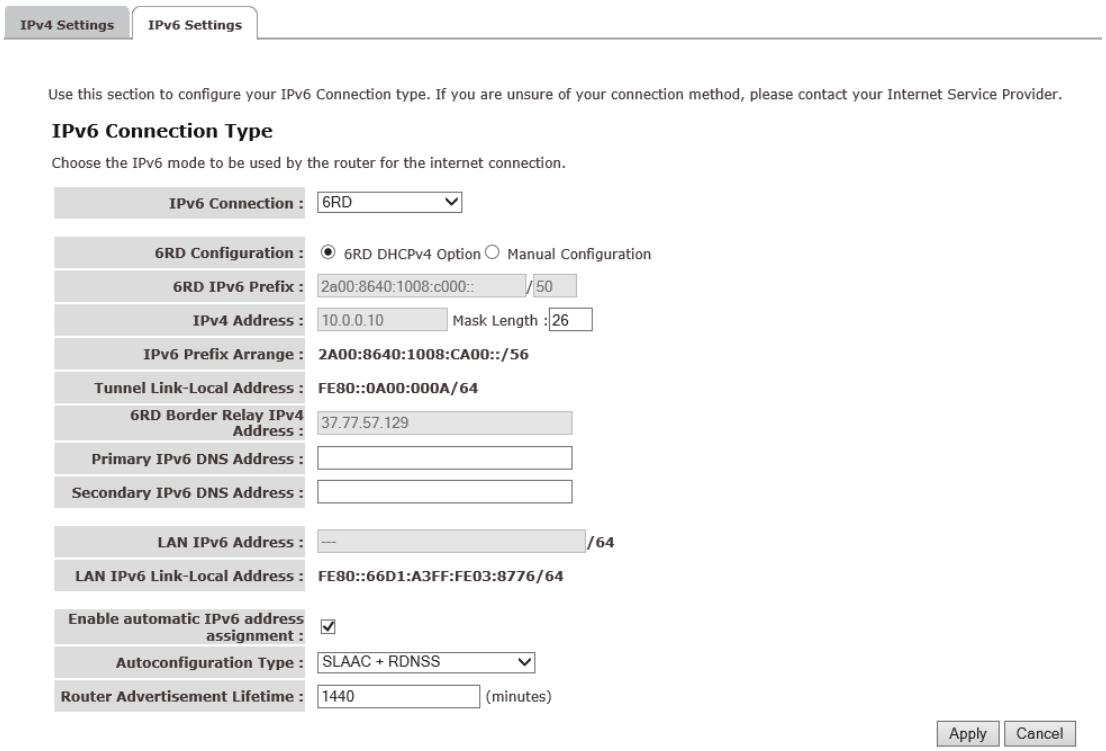
Static IPv6 Mode

This mode is used when your ISP provides you with a set IPv6 addresses that does not change. The IPv6 information is manually entered in your IPv6 configuration settings. You must enter the IPv6 address, Subnet Prefix Length, Default Gateway, Primary DNS Server and Secondary DNS Server. Your ISP provides you with all this information.


IPv4 Settings
IPv6 Settings
Use this section to configure your IPv6 Connection type. If you are unsure of your connection method, please contact your Internet Service Provider.
IPv6 Connection Type
Choose the IPv6 mode to be used by the router for the internet connection.
IPv6 Connection :
Static IPv6
Use Link-Local Address :
IPv6 Address :
Subnet Prefix Length :
0
Default Gateway :
Primary IPv6 DNS Address :
Secondary IPv6 DNS Address :
LAN IPv6 Address :
/64
LAN IPv6 Link-Local Address :
FE80::66D1:A3FF:FE03:8776/64
Enable automatic IPv6 address assignment :
Autoconfiguration Type :
SLAAC + RDNSS
Router Advertisement Lifetime :
1440
(minutes)

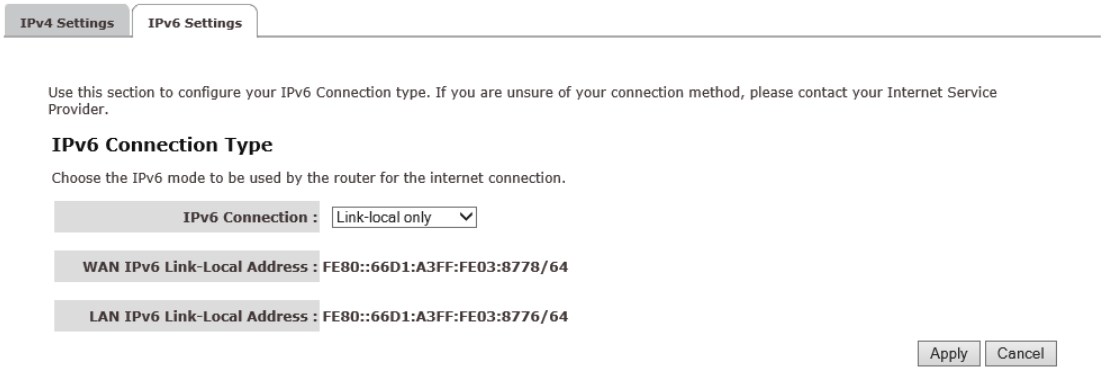
6RD Mode

In the 6RD mode, no additional configuration is necessary.



Link-local Mode

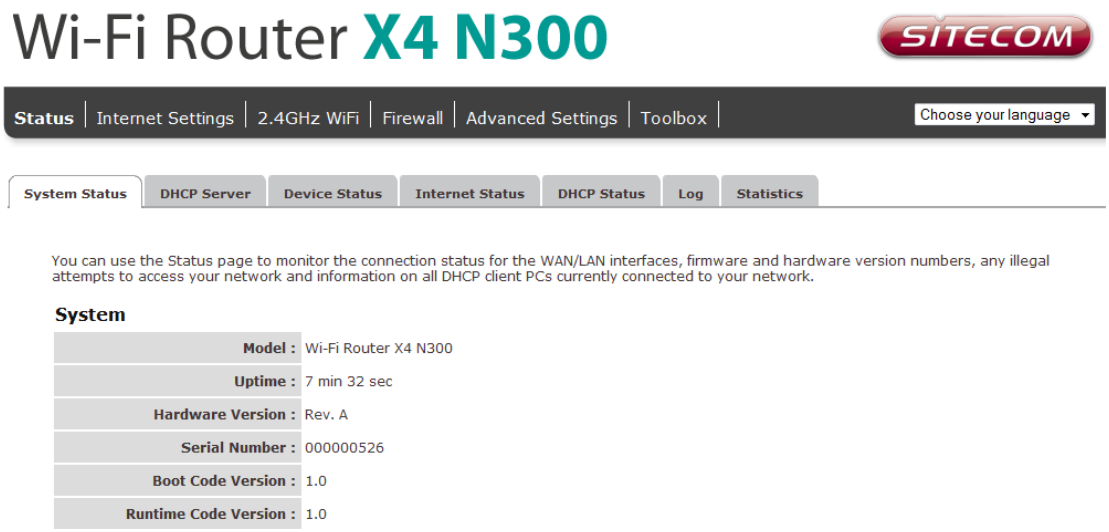
The Link-local address is used by nodes and routers when communicating with neighboring nodes on the same link. This mode enables IPv6-capable devices to communicate with each other on the LAN side.


IPv4 Settings
IPv6 Settings
Use this section to configure your IPv6 Connection type. If you are unsure of your connection method, please contact your Internet Service Provider.
IPv6 Connection Type
Choose the IPv6 mode to be used by the router for the internet connection.
IPv6 Connection :
Link-local only
WAN IPv6 Link-Local Address :
FE80::66D1:A3FF:FE03:8778/64
LAN IPv6 Link-Local Address :
FE80::66D1:A3FF:FE03:8776/64
Apply
Cancel

Configure your Router

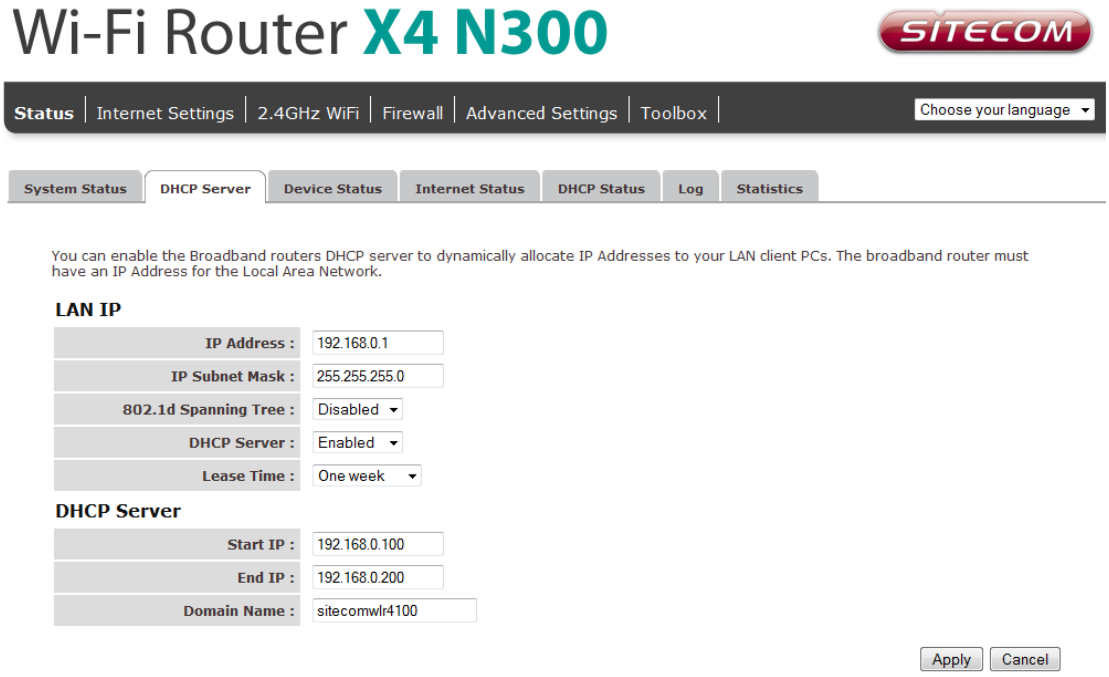
Status

The System status section allows you to monitor the current status of your router, the UP time, hardware information and serial number as well as firmware version information is displayed here.


Wi-Fi Router X4 N300
SITECOM
Status
Internet Settings
2.4GHz WiFi
Firewall
Advanced Settings
Toolbox
Choose your language
System Status
DHCP Server
Device Status
Internet Status
DHCP Status
Log
Statistics
You can use the Status page to monitor the connection status for the WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network and information on all DHCP client PCs currently connected to your network.
System
Model : Wi-Fi Router X4 N300
Uptime : 7 min 32 sec
Hardware Version : Rev. A
Serial Number : 000000526
Boot Code Version : 1.0
Runtime Code Version : 1.0

DHCP Server

The DHCP Server tab gives you the opportunity to change the IP settings of the router.

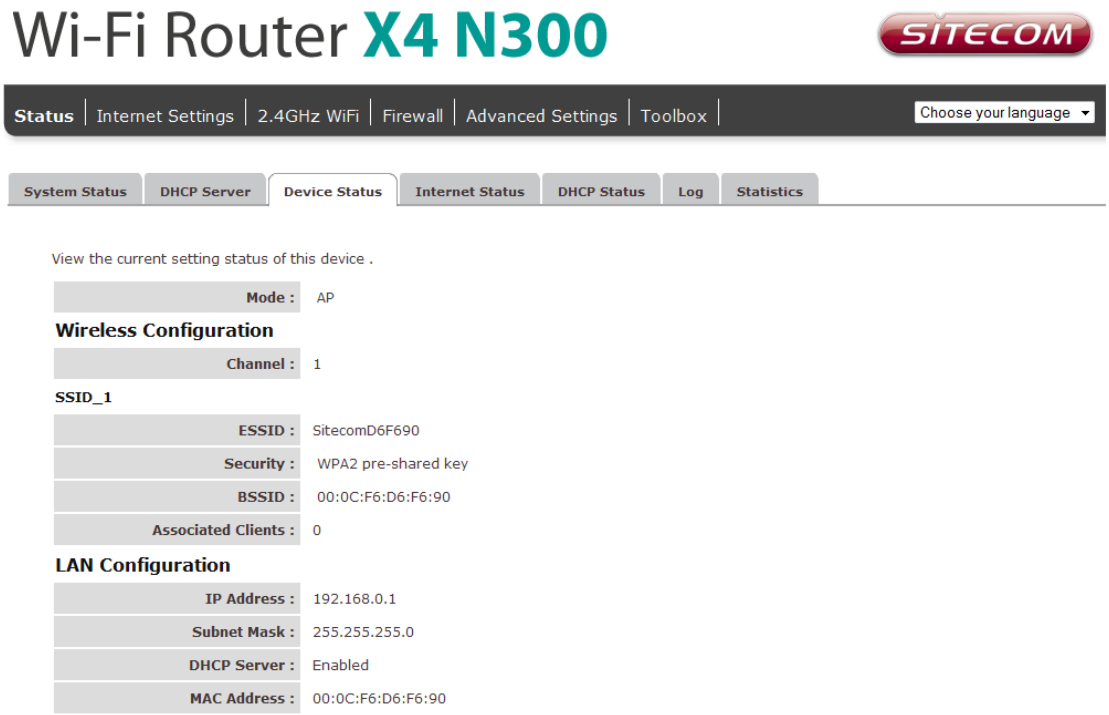


Click **Apply** at the bottom of this screen to save any changes.

- **IP address 192.168.0.1**: It is the router's LAN IP address (Your LAN clients default gateway IP address).
- **IP Subnet Mask 255.255.255.0**: Specify a Subnet Mask for your LAN segment.
- **802.1d Spanning Tree**: Disabled by default. If the 802.1d Spanning Tree function is enabled, this router will use the spanning tree protocol to prevent network loops.
- **DHCP Server**: Enabled by default. You can enable or disable the DHCP server. When DHCP is disabled no ip-addresses are assigned to clients and you have to use static ip-addresses. When DHCP server is enabled your computers will be assigned an ip-address automatically until the lease time expires.
- **Lease Time**: One Week. In the Lease Time setting you can specify the time period that the DHCP lends an IP address to your LAN clients. The DHCP will change your LAN client's IP address when this time threshold period is reached.
- **IP Address Pool**: You can select a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients. The default IP range is 192.168.0.100 ~ 192.168.0.200. If you want your PC(s) to have a static/fixed IP address, then you'll have to choose an IP address outside this IP address Pool
- **Domain Name**: You can specify a Domain Name for your LAN or just keep the default (sitecomwlr4100).

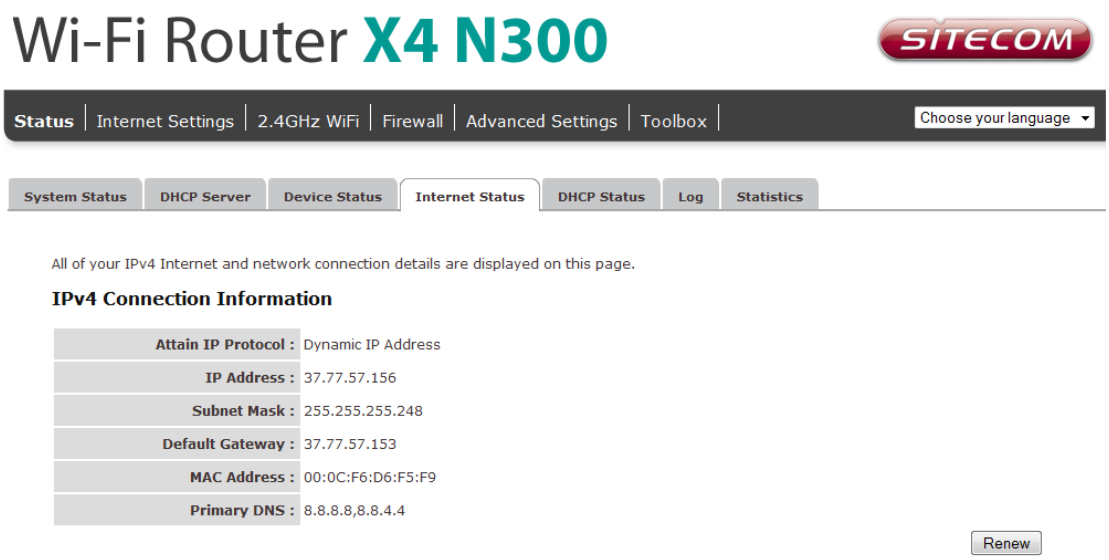
Device Status

View the router's current configuration settings. Device Status displays the configuration settings you've configured in the Internet Settings and WiFi Settings sections.



Internet Status

This page displays whether the WAN port is connected to a Cable/DSL connection. It also displays the router's WAN IP address, Subnet Mask, and ISP Gateway as well as MAC address, the Primary DNS. Press Renew button to renew your WAN IP address.

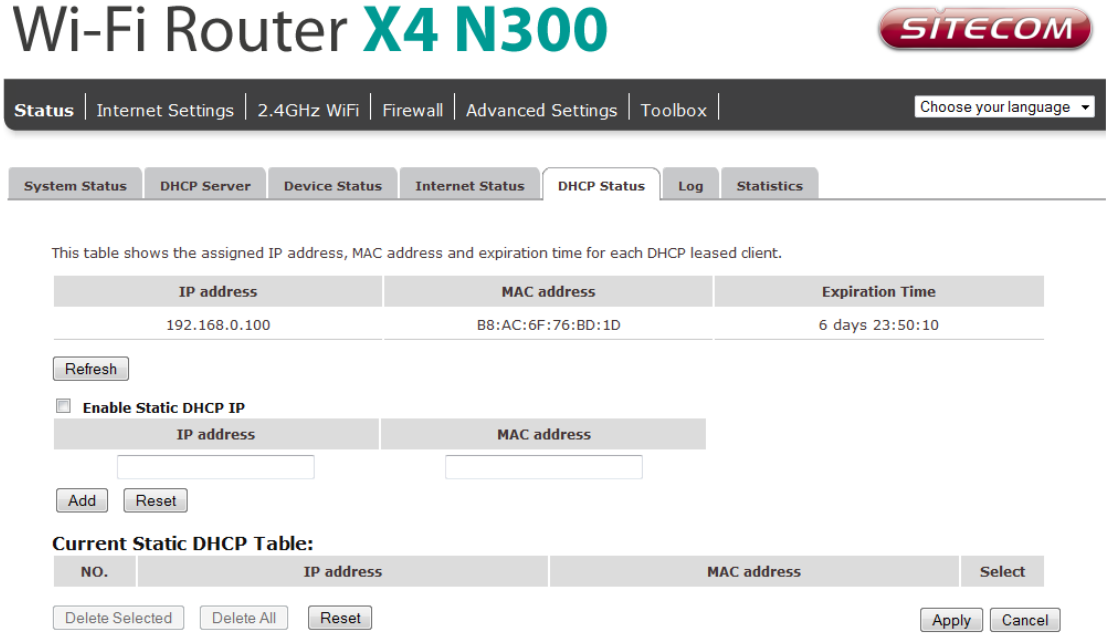


DHCP Client Status

This page shows all DHCP clients (LAN PCs) currently connected to your network. The table shows the assigned IP address, MAC address and expiration time for each DHCP leased client. Use the Refresh button to update the available information.

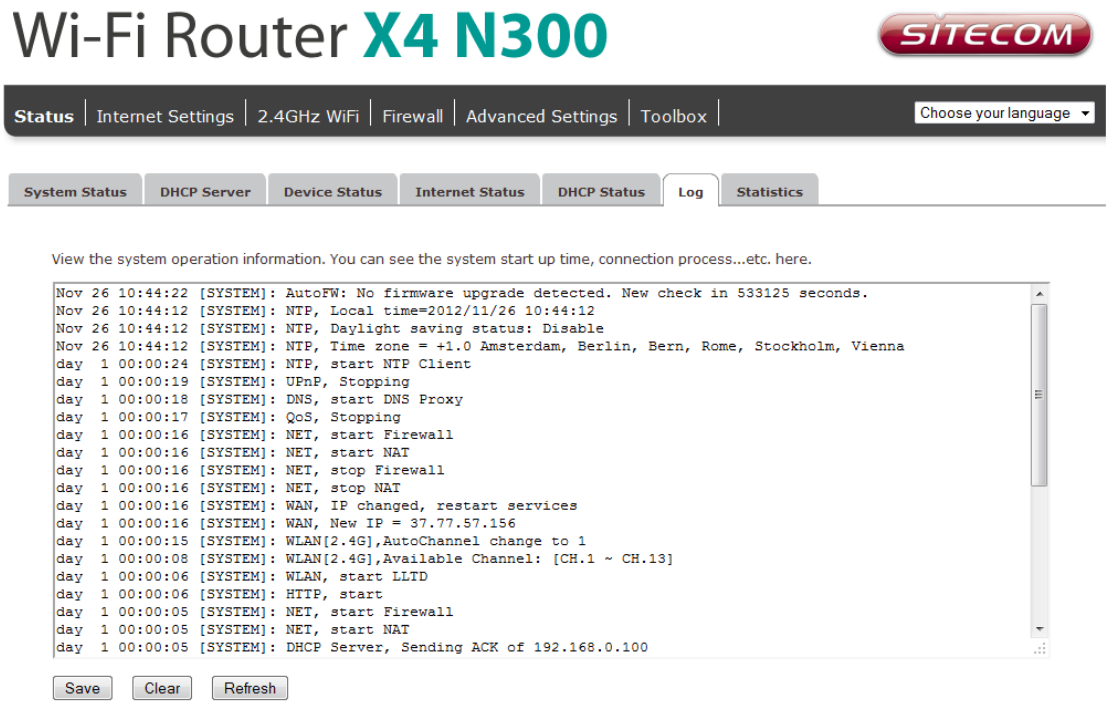
You can check "Enable Static DHCP IP". It is possible to add more static DHCP IPs. They are listed in the table Current Static DHCP Table. IP can be deleted at will from the table.

Click **Apply** to save the changed configuration.



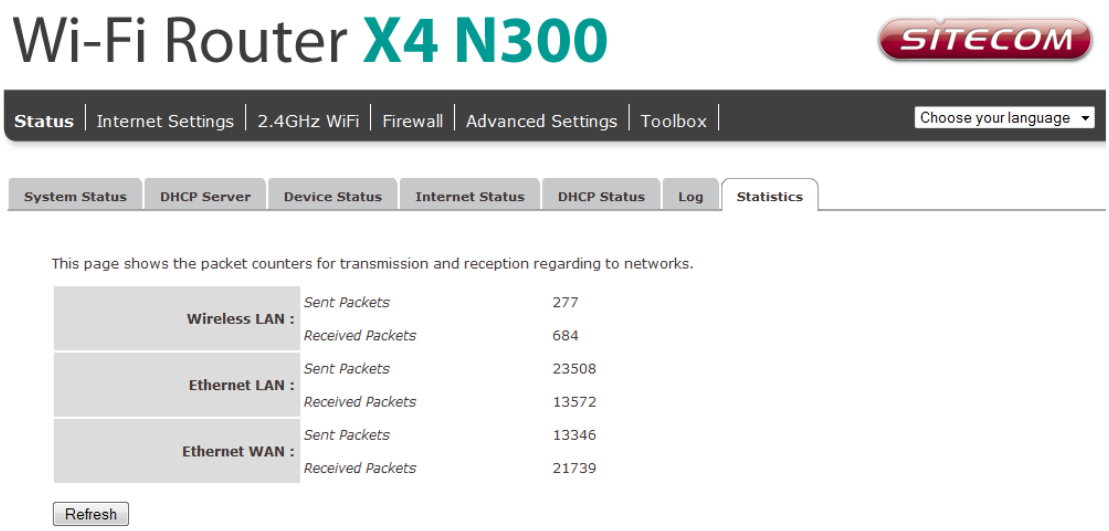
Log

View the operation log of the router. This page shows the current system log of the router. It displays any event that occurred during or after system start up. At the bottom of the page, the system log can be saved <Save> to a local file for further processing or the system log can be cleared <Clear> or it can be refreshed <Refresh> to get the most updated information. When the system is powered down, the system log will disappear if not saved to a local file.


Wi-Fi Router X4 N300
SITECOM
Status
Internet Settings
2.4GHz WiFi
Firewall
Advanced Settings
Toolbox
Choose your language
System Status
DHCP Server
Device Status
Internet Status
DHCP Status
Log
Statistics
View the system operation information. You can see the system start up time, connection process...etc. here.
Nov 26 10:44:22 [SYSTEM]: AutoFW: No firmware upgrade detected. New check in 533125 seconds.
Nov 26 10:44:12 [SYSTEM]: NTP, Local time=2012/11/26 10:44:12
Nov 26 10:44:12 [SYSTEM]: NTP, Daylight saving status: Disable
Nov 26 10:44:12 [SYSTEM]: NTP, Time zone = +1.0 Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
day 1 00:00:24 [SYSTEM]: NTP, start NTP Client
day 1 00:00:19 [SYSTEM]: UPnP, Stopping
day 1 00:00:18 [SYSTEM]: DNS, start DNS Proxy
day 1 00:00:17 [SYSTEM]: QoS, Stopping
day 1 00:00:16 [SYSTEM]: NET, start Firewall
day 1 00:00:16 [SYSTEM]: NET, start NAT
day 1 00:00:16 [SYSTEM]: NET, stop Firewall
day 1 00:00:16 [SYSTEM]: NET, stop NAT
day 1 00:00:16 [SYSTEM]: WAN, IP changed, restart services
day 1 00:00:16 [SYSTEM]: WAN, New IP = 37.77.57.156
day 1 00:00:15 [SYSTEM]: WLAN[2.4G],AutoChannel change to 1
day 1 00:00:08 [SYSTEM]: WLAN[2.4G],Available Channel: [CH.1 ~ CH.13]
day 1 00:00:06 [SYSTEM]: WLAN, start LLTD
day 1 00:00:06 [SYSTEM]: HTTP, start
day 1 00:00:05 [SYSTEM]: NET, start Firewall
day 1 00:00:05 [SYSTEM]: NET, start NAT
day 1 00:00:05 [SYSTEM]: DHCP Server, Sending ACK of 192.168.0.100
Save
Clear
Refresh

Statistics

Shows the counters of packets sent and received on WAN, LAN & WLAN.



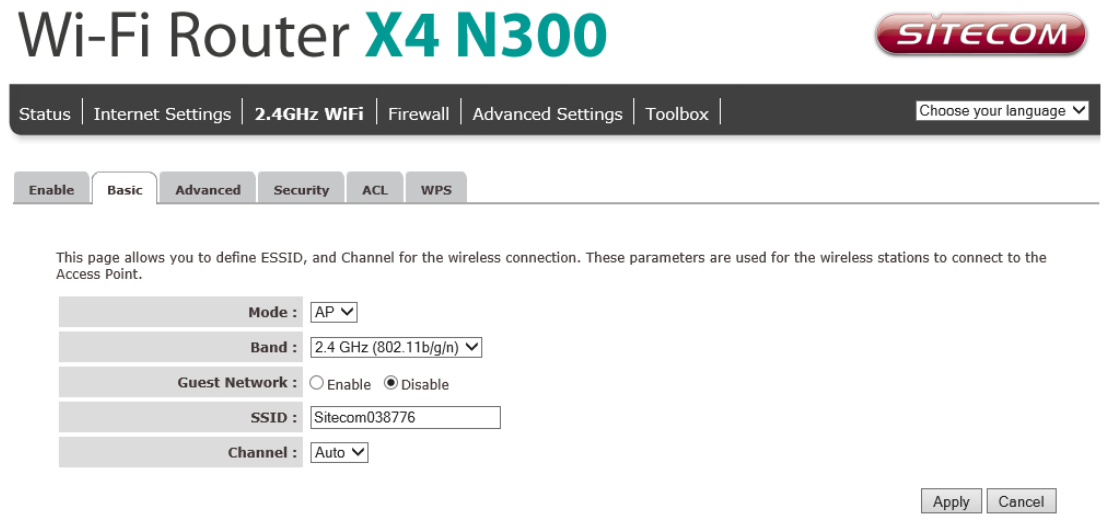
Wireless Settings

You can set parameters that are used for the wireless stations to connect to this router. The parameters include Mode, ESSID, Channel Number and Associated Client.

Wireless Function

Enable or Disable Wireless function here. Click Apply and wait for module to be ready & loaded.

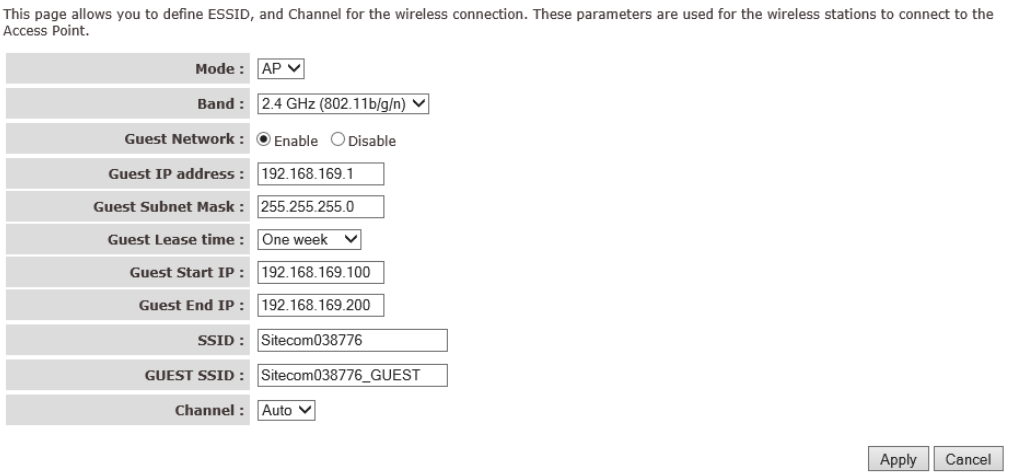
Basic Settings



- **Band**: Allows you to set the AP fixed at 802.11b or 802.11g mode. You can also select B+G mode to allow 802.11b and 802.11g clients at the same time.
- **Guest Network**: Enable this to activate the Guest Network. Devices connected to the Guest network will have Internet connection but no access to the main network and cannot communicate with each other

- **SSID**: This is the name of the wireless signal which is broadcasted. All the devices in the same wireless LAN should have the same SSID.
- **Channel**: The channel used by the wireless LAN. All devices in the same wireless LAN should use the same channel.

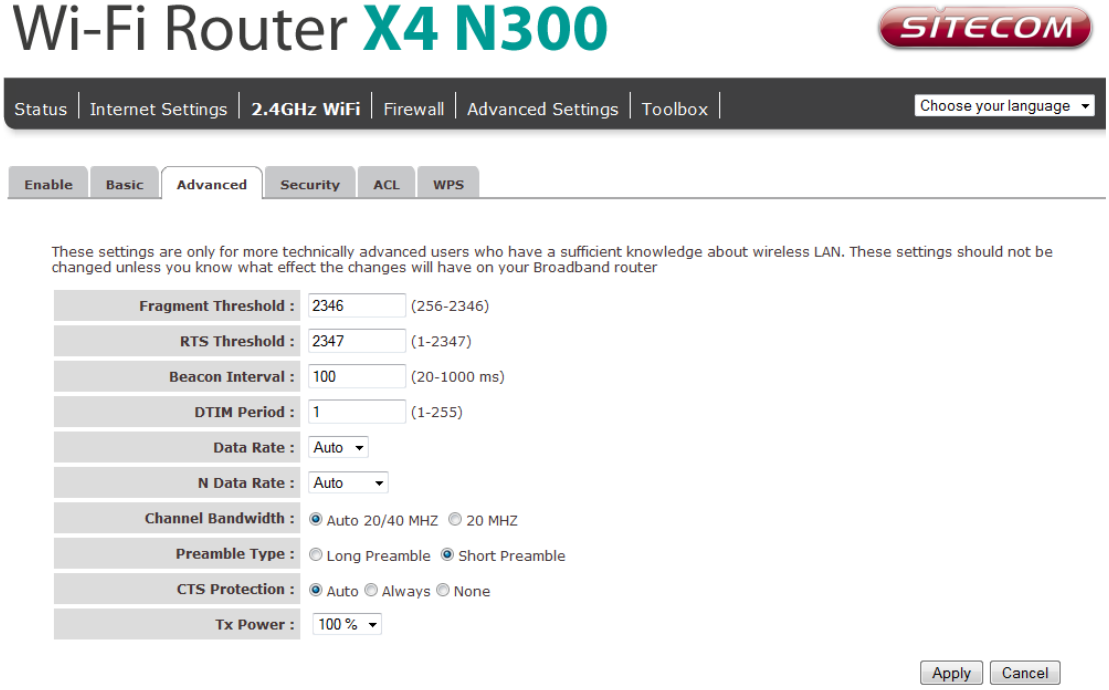
Guest Network (Firmware 2.0 and up only)


This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.
Mode : AP
Band : 2.4 GHz (802.11b/g/n)
Guest Network : Enable Disable
Guest IP address : 192.168.169.1
Guest Subnet Mask : 255.255.255.0
Guest Lease time : One week
Guest Start IP : 192.168.169.100
Guest End IP : 192.168.169.200
SSID : Sitecom038776
GUEST SSID : Sitecom038776_GUEST
Channel : Auto
Apply
Cancel

- **Guest IP address**: The gateway address for the Guest Network. This address cannot be the same as the default router's IP Address.
- **Guest Subnet Mask**: The Subnet Mask for the Guest network. This address cannot be the same as the default router's Subnet Mask.
- **Guest Lease Time**: One Week. In the Lease Time setting you can specify the time period that the DHCP lends an IP address to your LAN clients. The DHCP will change your LAN client's IP address when this time threshold period is reached.
- **Guest Start IP + End IP**: You can select a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients. The default IP range is 192.168.169.100 ~ 192.168.169.200. This address pool cannot be the same as the default router's DHCP Address pool.
- **Guest SSID**: This is the name of the wireless signal which is broadcasted as the Guest Network. This name cannot be the same as the default SSID.

Advanced Settings

This tab allows you to set the advanced wireless options. The options included are Authentication Type, Fragment Threshold, RTS Threshold, Beacon Interval, and Preamble Type. You should not change these parameters unless you know what effect the changes will have on the router.


Wi-Fi Router X4 N300
SITECOM
Status | Internet Settings | 2.4GHz WiFi | Firewall | Advanced Settings | Toolbox
Choose your language
Enable | Basic | Advanced | Security | ACL | WPS
These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Broadband router
Fragment Threshold : 2346 (256-2346)
RTS Threshold : 2347 (1-2347)
Beacon Interval : 100 (20-1000 ms)
DTIM Period : 1 (1-255)
Data Rate : Auto
N Data Rate : Auto
Channel Bandwidth : Auto 20/40 MHZ 20 MHZ
Preamble Type : Long Preamble Short Preamble
CTS Protection : Auto Always None
Tx Power : 100 %
Apply
Cancel

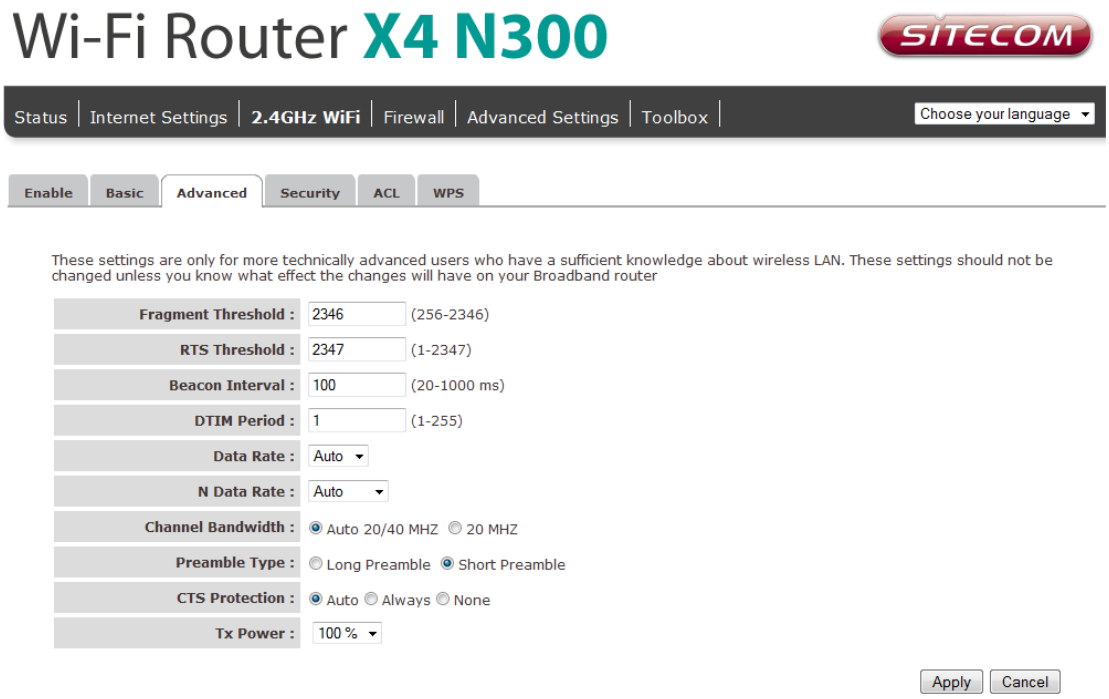
- **Authentication Type**: There are two authentication types: "Open System" and "Shared Key". When you select "Open System", wireless stations can associate with this wireless router without WEP encryption. When you select "Shared Key", you should also setup a WEP key in the "Encryption" page. After this has been done, make sure the wireless clients that you want to connect to the device are also setup with the same encryption key.
- **Fragment Threshold**: "Fragment Threshold" specifies the maximum size of a packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.
- **RTS Threshold**: When the packet size is smaller then the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.
- **Beacon Interval**: This is the interval of time that this wireless router broadcasts a beacon. A Beacon is used to synchronize the wireless network.
- **Data Rate**: The "Data Rate" is the rate that this access point uses to transmit data packets. The access point will use the highest possible selected transmission rate to transmit the data packets.
- **N Data Rate**: The "Data Rate" is the rate that this access point uses to transmit data packets for N compliant wireless nodes. Highest to lowest data rate can be fixed.
- **Channel Bandwidth**: This is the range of frequencies that will be used.
- **Preamble Type**: The "Long Preamble" can provide better wireless LAN compatibility while the "Short Preamble" can provide better wireless LAN performance.
- **Broadcast ESSID**: If you enabled "Broadcast ESSID", every wireless station located within the coverage of this access point can discover this access point easily. If you are building a public wireless network, enabling this feature is recommended. Disabling "Broadcast ESSID" can provide better security.
- **CTS Protection**: It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the

throughput of the AP will be a little lower due to a lot of frame-network that is transmitted.

- **TX Power**: The transmit power can be set to a bare minimum or maximum power for better performance or power saving.
- **WMM**: WiFi Multi Media. If enabled this supports QoS for experiencing better audio, video and voice in applications.

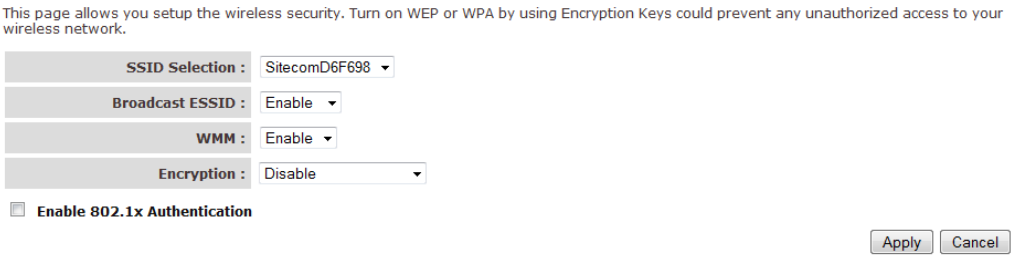
Security

This router provides complete wireless LAN security functions, included are WEP, IEEE 802.11x, IEEE 802.11x with WEP, WPA with pre-shared key and WPA with RADIUS. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security function, and are setup with the same security key.


Wi-Fi Router X4 N300
SITECOM
Status
Internet Settings
2.4GHz WiFi
Firewall
Advanced Settings
Toolbox
Choose your language
Enable
Basic
Advanced
Security
ACL
WPS
These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Broadband router
Fragment Threshold : 2346 (256-2346)
RTS Threshold : 2347 (1-2347)
Beacon Interval : 100 (20-1000 ms)
DTIM Period : 1 (1-255)
Data Rate : Auto
N Data Rate : Auto
Channel Bandwidth : Auto 20/40 MHZ 20 MHZ
Preamble Type : Long Preamble Short Preamble
CTS Protection : Auto Always None
Tx Power : 100 %
Apply
Cancel

Disable

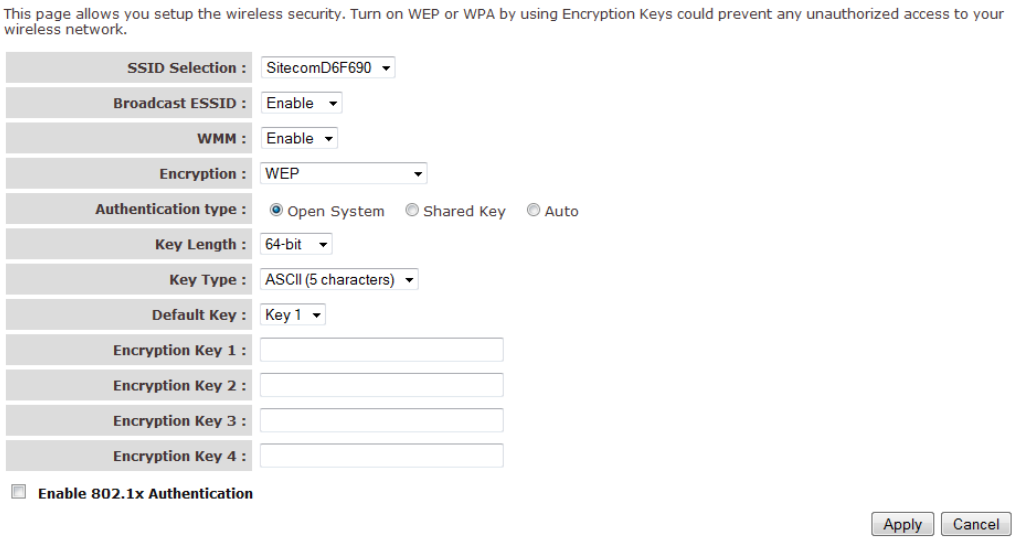
When you choose to disable encryption, it is very insecure to use the router.


This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.
SSID Selection : SitecomD6F698
Broadcast ESSID : Enable
WMM : Enable
Encryption : Disable
Enable 802.1x Authentication
Apply
Cancel

Enable 802.1x Authentication

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates users by IEEE 802.1x, but it does not encrypt the data during communication

WEP

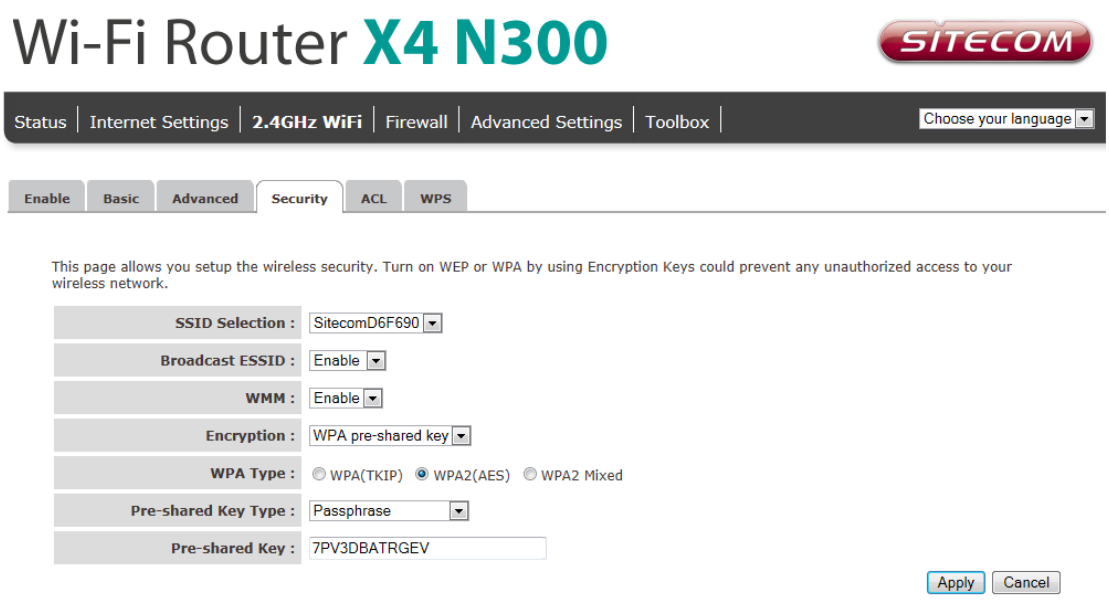


When you select 64-bit or 128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself and enter it. You can enter four WEP keys and select one of them as a default key. Then the router can receive any packets encrypted by one of the four keys.

- **Key Length**: You can select the WEP key length for encryption, 64-bit or 128-bit. The larger the key will be the higher level of security is used, but the throughput will be lower.
- **Key Type**: You may select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key.
- **Key1 - Key4**: The WEP keys are used to encrypt data transmitted in the wireless network. Use the following rules to setup a WEP key on the device. 64-bit WEP: input 10-digits Hex values (in the "A-F", "a-f" and "0-9" range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 13-digit ASCII characters as the encryption keys.

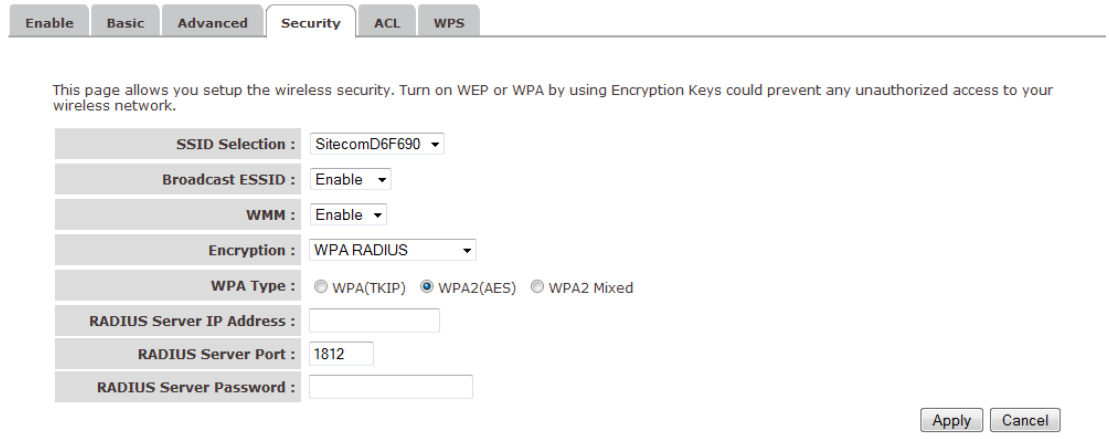
Click **Apply** at the bottom of the screen to save the above configuration.

WPA Pre-shared Key



Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently, so the encryption key is not easy to be cracked by hackers. This is the best security available.

WPA-Radius



Wi-Fi Protected Access (WPA) is an advanced security standard. You can use an external RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. Press **Apply** when you are done.

ACL

This wireless router supports MAC Address Control, which prevents unauthorized clients from accessing your wireless network.

- **Enable wireless access control**: Enables the wireless access control function
- **Adding an address into the list**: Enter the "MAC Address" and "Comment" of the wireless station to be added and then click "Add". The wireless station will now be added into the "Current Access Control List" below. If you are having any difficulties filling in the fields, just click "Clear" and both "MAC Address" and "Comment" fields will be cleared.
- **Remove an address from the list**: If you want to remove a MAC address from the "Current Access Control List ", select the MAC address that you want to remove in the list and then click "Delete Selected". If you want to remove all the MAC addresses from the list, just click the "Delete All" button. Click "Reset" will clear your current selections.

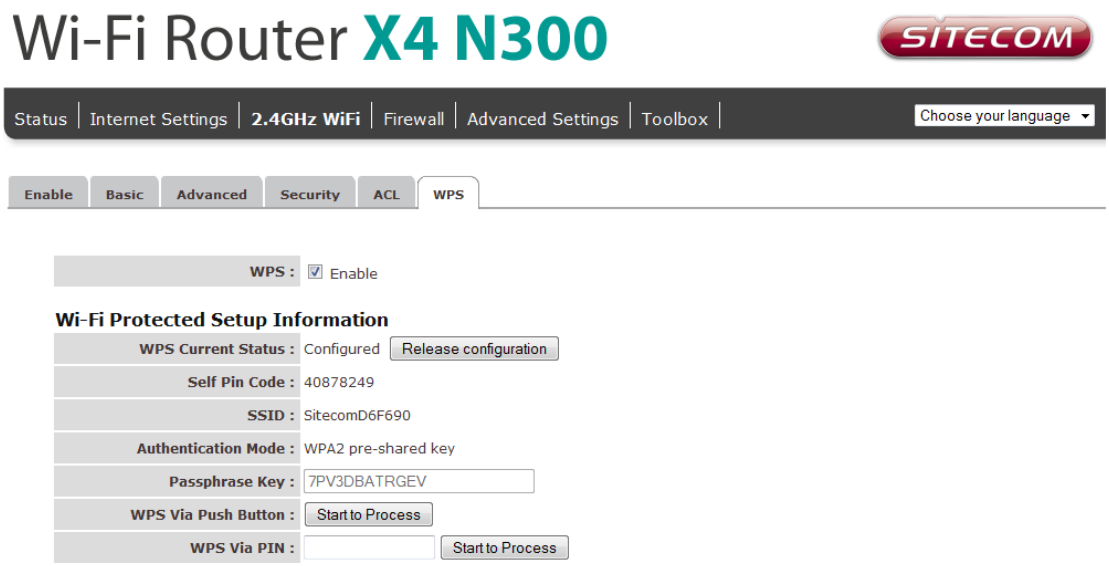
Click **Apply** at the bottom of the screen to save the above configurations. You can now configure other sections by choosing Continue, or choose Apply to apply the settings and reboot the device.

WPS

Wi-Fi Protected Setup (WPS) is the simplest way to establish a connection between the wireless clients and the wireless router. You don't have to select the encryption mode and fill in a long encryption passphrase every time when you try to setup a wireless connection. You only need to press a button on both wireless client and wireless router, and WPS will do the rest for you.

The wireless router supports two types of WPS: WPS via Push Button and WPS via PIN code. If you want to use the Push Button, you have to push a specific button on the wireless client or in the utility of the wireless client to start the WPS mode, and switch the wireless router to WPS mode. You can simply push the WPS button of the wireless router, or click the 'Start to Process' button in the web configuration interface. If you

want to use the PIN code, you have to know the PIN code of the wireless client and switch it to WPS mode, then fill-in the PIN code of the wireless client through the web configuration interface of the wireless router.

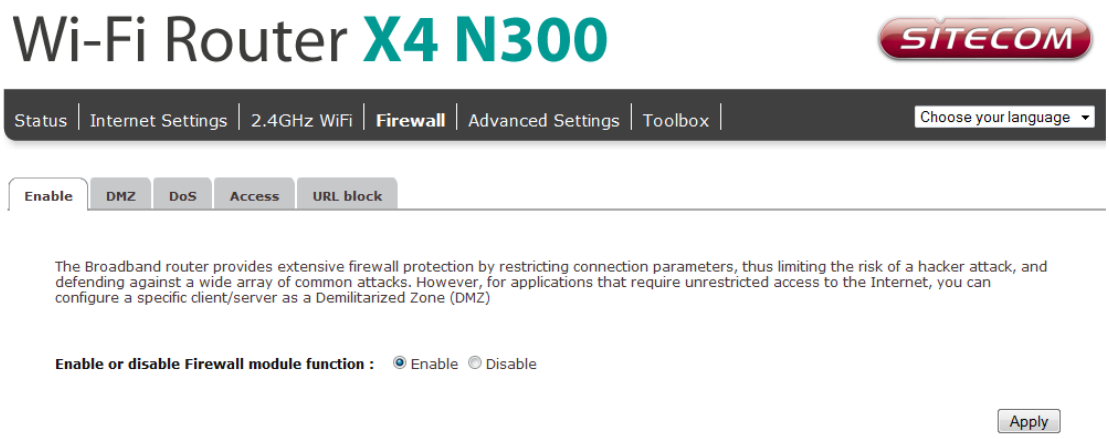


- **WPS**: Check the box to enable WPS function and uncheck it to disable the WPS function.
- **WPS Current Status**: If the wireless security (encryption) function of this wireless router is properly set, you'll see a 'Configured' message here. Otherwise, you'll see 'UnConfigured'.
- **Self-Pin Code**: This is the WPS PIN code of the wireless router. You may need this information when connecting to other WPS-enabled wireless devices.
- **SSID**: This is the network broadcast name (SSID) of the router.
- **Authentication Mode**: It shows the active authentication mode for the wireless connection.
- **Passphrase Key**: It shows the passphrase key that is randomly generated by the wireless router during the WPS process. You may need this information when using a device which doesn't support WPS.
- **WPS via Push Button**: Press the button to start the WPS process. The router will wait for the WPS request from the wireless devices within 2 minutes.
- **WPS via PIN**: You can fill-in the PIN code of the wireless device and press the button to start the WPS process. The router will wait for the WPS request from the wireless device within 2 minutes.

Firewall Settings

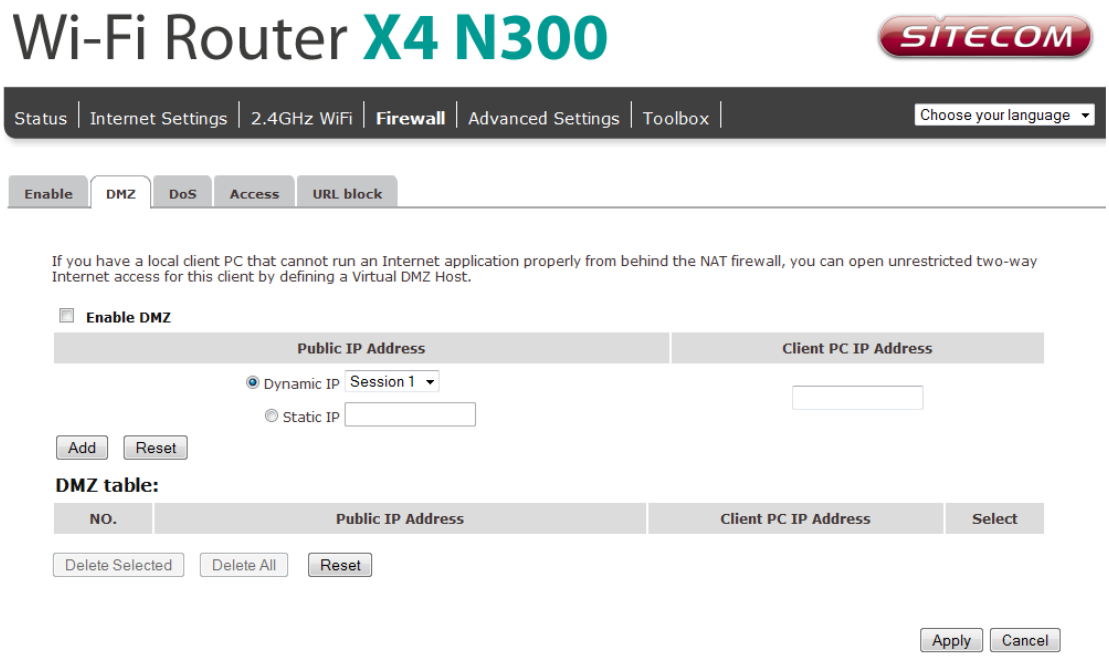
The router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attacks, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).

Note: To enable the Firewall settings select Enable and click **Apply**


Wi-Fi Router X4 N300
SITECOM
Status
Internet Settings
2.4GHz WiFi
Firewall
Advanced Settings
Toolbox
Choose your language
Enable
DMZ
DoS
Access
URL block
The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of a hacker attack, and defending against a wide array of common attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ)
Enable or disable Firewall module function :
Enable
Disable
Apply

DMZ

If you have a client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, then you can open up the firewall restrictions to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all packets going to your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) going to your WAN IP address to a particular LAN client/server.

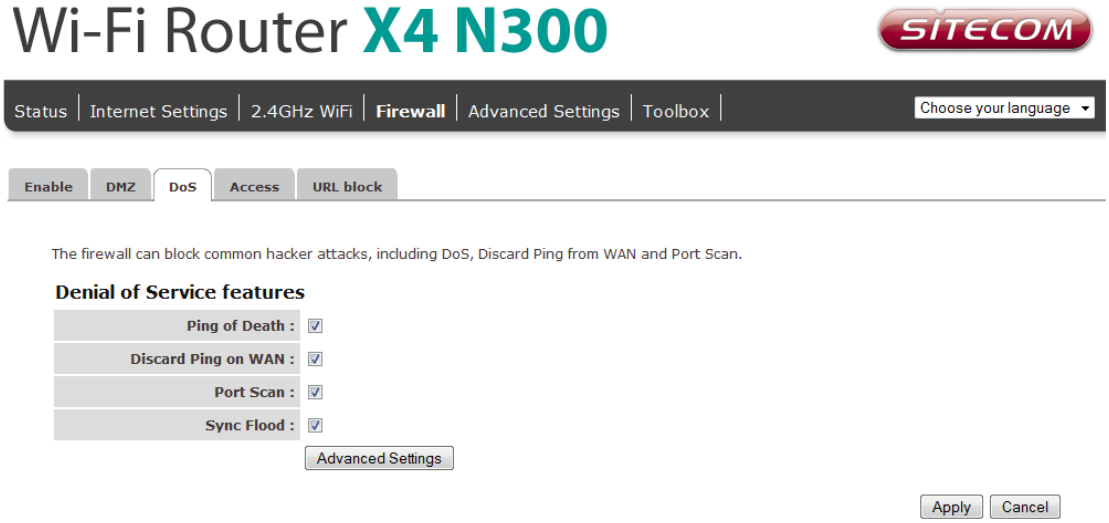

Wi-Fi Router X4 N300
SITECOM
Status | Internet Settings | 2.4GHz WiFi | Firewall | Advanced Settings | Toolbox
Choose your language
Enable | DMZ | DoS | Access | URL block
If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, you can open unrestricted two-way Internet access for this client by defining a Virtual DMZ Host.
Enable DMZ
Public IP Address
Client PC IP Address
Dynamic IP
Session 1
Static IP
Add
Reset
DMZ table:
NO.
Public IP Address
Client PC IP Address
Select
Delete Selected
Delete All
Reset
Apply
Cancel

- **Enable DMZ**: Enable/disable DMZ
- **Public IP Address**: The IP address of the WAN port or any other Public IP addresses given to you by your ISP
- **Client PC IP Address**: Fill-in the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/Public IP address above.

Click **Apply** at the bottom of the screen to save the above configurations.

Denial of Service (DoS)

The Broadband router's firewall can block common hacker attacks, including Denial of Service, Ping of Death, Port Scan and Sync Flood. If Internet attacks occur the router can log the events.

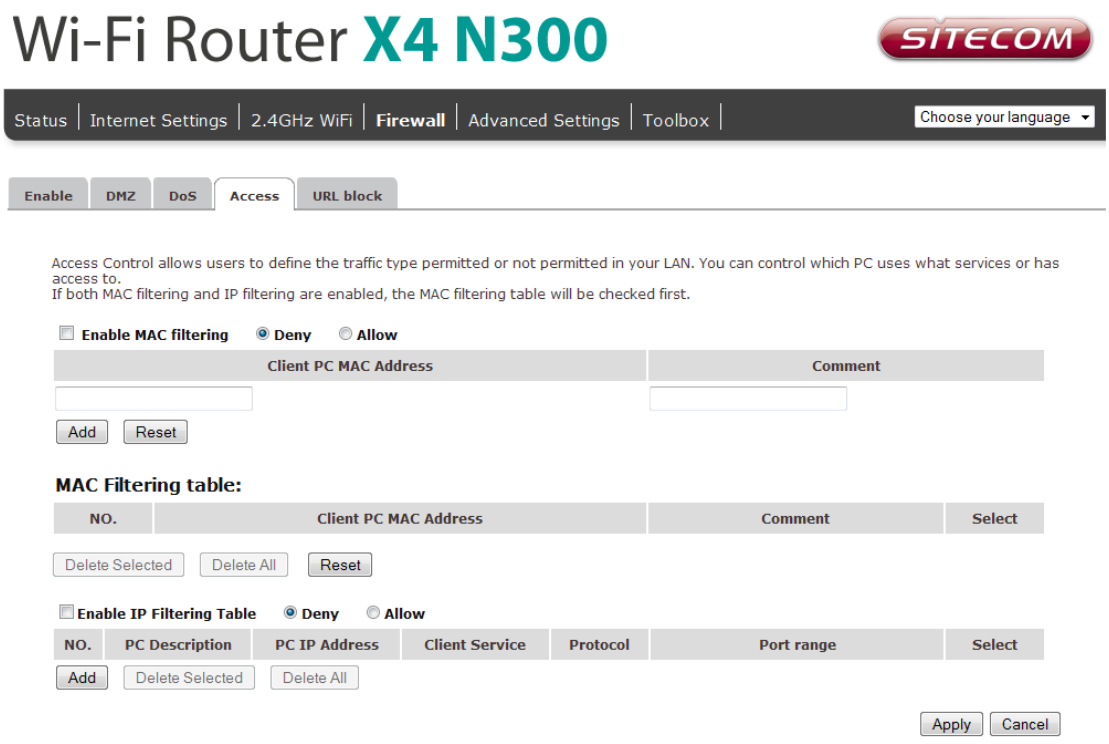

Wi-Fi Router X4 N300
SITECOM
Status | Internet Settings | 2.4GHz WiFi | Firewall | Advanced Settings | Toolbox
Choose your language
Enable | DMZ | DoS | Access | URL block
The firewall can block common hacker attacks, including DoS, Discard Ping from WAN and Port Scan.
Denial of Service features
Ping of Death :
Discard Ping on WAN :
Port Scan :
Sync Flood :
Advanced Settings
Apply
Cancel

- **Ping of Death**: Protection from Ping of Death attacks
- **Discard Ping From WAN**: The router's WAN port will not respond to any Ping requests
- **Port Scan**: Protects the router from Port Scans.
- **Sync Flood**: Protects the router from Sync Flood attack.

Click **Apply** at the bottom of the screen to save the above configuration.

Access

You can restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.), Access Control allows users to define the traffic type permitted in your LAN. You can control which PC client can have access to these services.



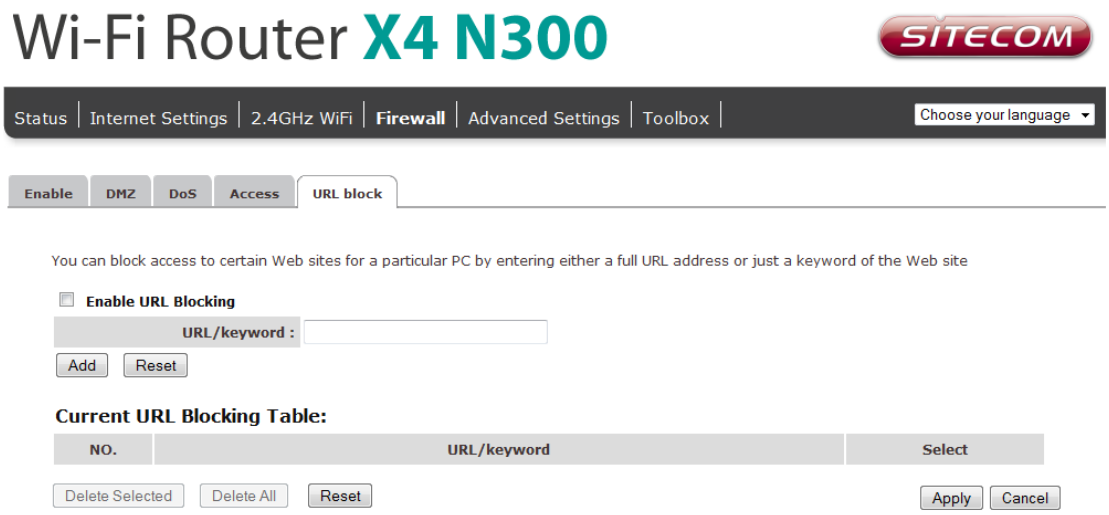
- **Deny**: If you select "Deny" then all clients will be allowed to access Internet accept for the clients in the list below.
- **Allow**: If you select "Allow" then all clients will be denied to access Internet accept for the PCs in the list below.
- **Filter client PCs by IP**: Fill in "IP Filtering Table" to filter PC clients by IP.
- **Add PC**: You can click Add PC to add an access control rule for users by IP addresses.
- **Remove PC**: If you want to remove some PCs from the "IP Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want to remove all PCs from the table, just click the "Delete All" button.
- **Filter client PC by MAC**: Check "Enable MAC Filtering" to enable MAC Filtering.
- **Add PC**: Fill in "Client PC MAC Address" and "Comment" of the PC that is allowed to access the Internet, and then click "Add". If you find any typo before adding it and want to retype again, just click "Reset" and the fields will be cleared.

- **Remove PC**: If you want to remove some PC from the "MAC Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want to remove all PCs from the table, just click the "Delete All" button. If you want to clear the selection and re-select again, just click “Reset”.

Click **Apply** at the bottom of the screen to save the above configuration.

URL block

You can block access to some Web sites from particular PCs by entering a full URL address or just keywords of the Web site.

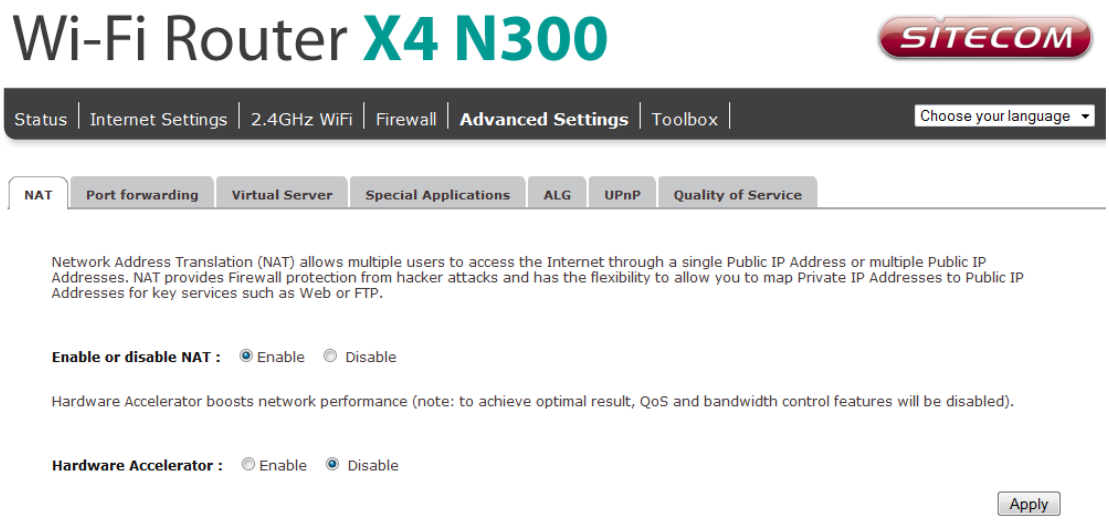


- **Enable**: URL Blocking Enable/disable URL Blocking
- **Add URL/keyword**: Fill in “URL/Keyword” and then click “Add”. You can enter the full URL address or the keyword of the web site you want to block.
- **Remove URL/keyword**: If you want to remove some URL keywords from the "Current URL Blocking Table", select the URL keyword you want to remove in the table and then click "Delete Selected". If you want remove all URL keywords from the table, just click "Delete All" button. If you want to clear the selection and re-select again, just click “Reset”.

Click **Apply** at the bottom of the screen to save the above configuration.

Advanced Settings

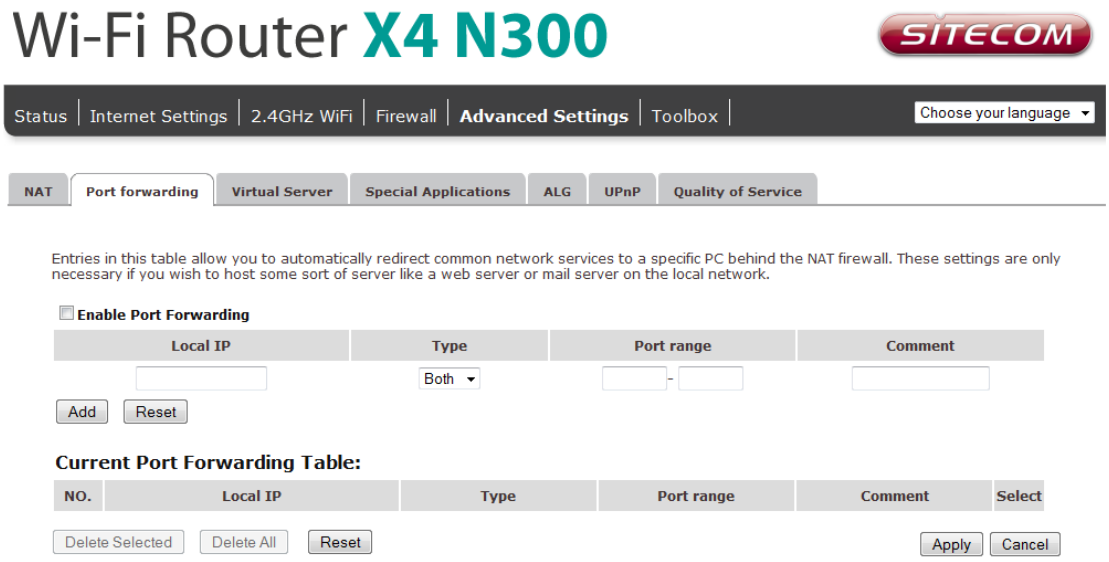
Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as Websites and FTP.


Wi-Fi Router X4 N300
SITECOM
Status
Internet Settings
2.4GHz WiFi
Firewall
Advanced Settings
Toolbox
Choose your language
NAT
Port forwarding
Virtual Server
Special Applications
ALG
UPnP
Quality of Service
Network Address Translation (NAT) allows multiple users to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as Web or FTP.
Enable or disable NAT :
Enable
Disable
Hardware Accelerator boosts network performance (note: to achieve optimal result, QoS and bandwidth control features will be disabled).
Hardware Accelerator :
Enable
Disable
Apply

Select **Disable** to disable the NAT function.

Port Forwarding

Port Forwarding allows you to re-direct a particular range of service port numbers (from the Internet/WAN Port) to a particular LAN IP address. It helps you to host servers behind the router NAT firewall.

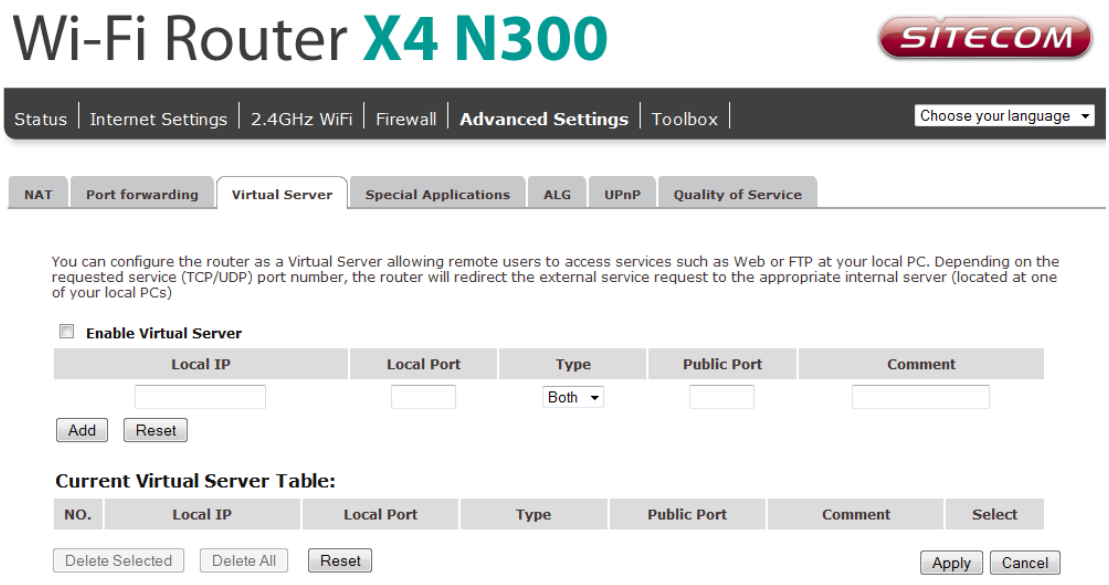


- **Enable Port Forwarding**: Enable Port Forwarding
- **Local IP**: This is the private IP of the server behind the NAT firewall.
- **Type**: This is the protocol type to be forwarded. You can choose to forward "TCP" or "UDP" packets only, or select "both" to forward both "TCP" and "UDP" packets.
- **Port Range**: The range of ports to be forward to the private IP.
- **Comment**: description of this setting.
- **Add**: Fill in the "Private IP", "Type", "Port Range" and "Comment" of the setting to be added and then click "Add". Then this Port Forwarding setting will be added into the "Current Port Forwarding Table" below.
- **Remove**: If you want to remove a Port Forwarding setting from the "Current Port Forwarding Table", select the Port Forwarding setting that you want to remove in the table and then click "Delete Selected". If you want to remove all Port Forwarding settings from the table, just click "Delete All" button. Click "Reset" will clear your current selections.

Click **Apply** at the bottom of the screen to save the above configuration.

Virtual Server

Use the Virtual Server function when you want different servers/clients in your LAN to handle different service/Internet application type (e.g. Email, FTP, Web server etc.) from the Internet. Computers use numbers called port numbers to recognize a particular service/Internet application type. The Virtual Server allows you to re-direct a particular service port number (from the Internet/WAN Port) to a particular LAN private IP address and its service port number.



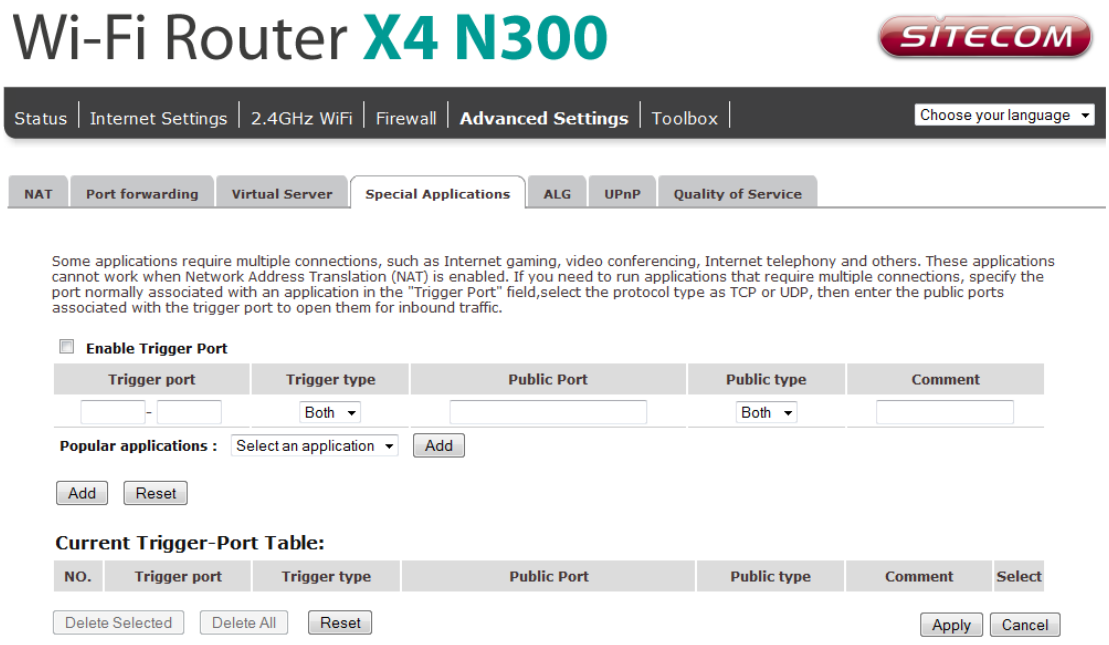
- **Enable Virtual Server**: Enable Virtual Server.
- **Local IP**: This is the LAN client/host IP address that the Public Port number packet will be sent to.
- **Local Port**: This is the port number (of the above Private IP host) that the below Public Port number will be changed to when the packet enters your LAN (to the LAN Server/Client IP).

- **Type**: Select the port number protocol type (TCP, UDP or both). If you are unsure, then leave it to the default “both” setting. Public Port Enter the service (service/Internet application) port number from the Internet that will be re-directed to the above Private IP address host in your LAN
- **Comment**: The description of this setting.
- **Add**: Fill in the "Private IP", "Private Port", "Type", “Public Port” and "Comment" of the setting to be added and then click "Add". Then this Virtual Server setting will be added into the "Current Virtual Server Table" below.
- **Reset**: If you want to remove Virtual Server settings from the "Current Virtual Server Table", select the Virtual Server settings you want to remove in the table and then click "Delete Selected". If you want to remove all Virtual Server settings from the table, just click the "Delete All" button. Click "Reset" will clear your current selections.

Click **Apply** at the bottom of the screen to save the above configuration.

Special Applications

Some applications require multiple connections, such as Internet games, video Conferencing, Internet telephony and others. In this section you can configure the router to support multiple connections for these types of applications.



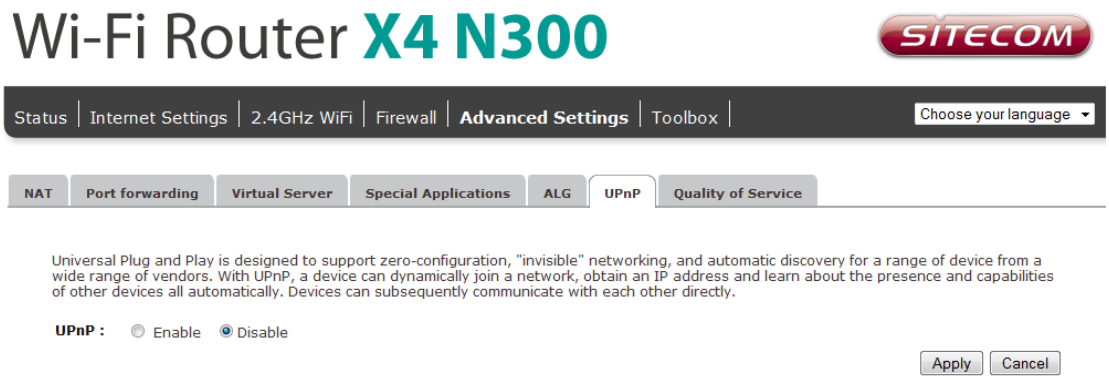
- **Enable Trigger Port**: Enable the Special Application function.
- **Trigger Port**: This is the outgoing (Outbound) range of port numbers for this particular application.
- **Trigger Type**: Select whether the outbound port protocol is “TCP”, “UDP” or both.
- **Public Port**: Enter the In-coming (Inbound) port or port range for this type of application (e.g. 2300-2400, 47624).
- **Public Type**: Select the Inbound port protocol type: “TCP”, “UDP” or both.
- **Comment**: The description of this setting.

- **Popular applications**: This section lists the more popular applications that require multiple connections. Select an application from the Popular Applications selection. Once you have selected an application, select a location (1-10) in the Copy to selection box and then click the Copy to button. This will automatically list the Public Ports required for this popular application in the location (1-10) you specified.
- **Add**: Fill in the "Trigger Port", "Trigger Type", "Public Port", "Public Type", "Public Port" and "Comment" of the setting to be added and then click "Add". The Special Application setting will be added into the "Current Trigger-Port Table" below. If you happen to make a mistake, just click "Clear" and the fields will be cleared.
- **Reset**: If you want to remove Special Application settings from the "Current Trigger-Port Table", select the Special Application settings you want to remove in the table and then click "Delete Selected". If you want remove all Special Application settings from the table, just click the "Delete All" button. Click "Reset" will clear your current selections.

Click **Apply** at the bottom of the screen to save the above configuration.

UPnP

With UPnP, all PCs in you Intranet will discover this router automatically, so you don't have to configure your PC and it can easily access the Internet through this router.


Wi-Fi Router X4 N300
SITECOM
Status
Internet Settings
2.4GHz WiFi
Firewall
Advanced Settings
Toolbox
Choose your language
NAT
Port forwarding
Virtual Server
Special Applications
ALG
UPnP
Quality of Service
Universal Plug and Play is designed to support zero-configuration, "invisible" networking, and automatic discovery for a range of device from a wide range of vendors. With UPnP, a device can dynamically join a network, obtain an IP address and learn about the presence and capabilities of other devices all automatically. Devices can subsequently communicate with each other directly.
UPnP :
Enable
Disable
Apply
Cancel

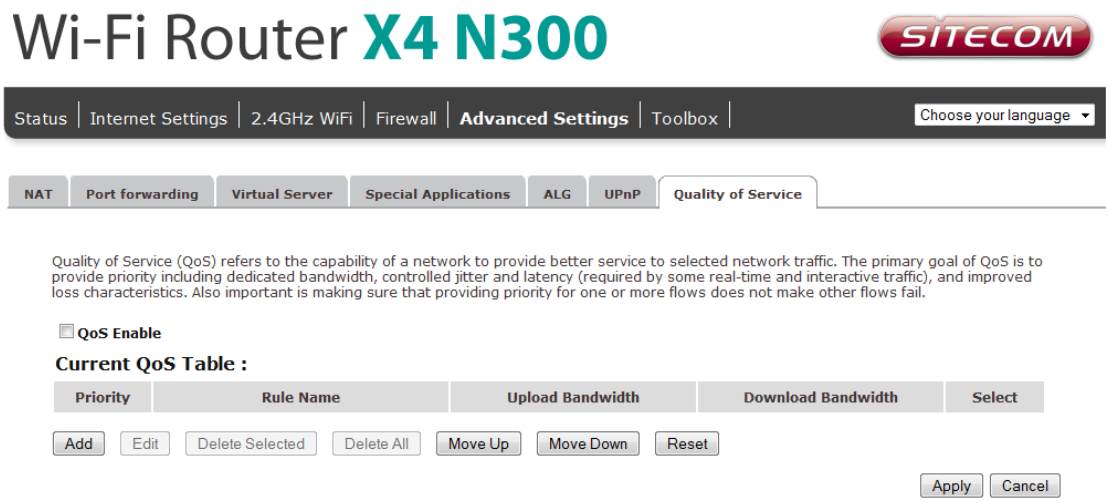
UPnP Feature: You can enable or Disable the UPnP feature here. After you enable the UPnP feature, all client systems that support UPnP, like Windows XP, can discover this router automatically and access the Internet through this router without having to configure anything. The NAT Traversal function provided by UPnP can let applications that support UPnP connect to the internet without having to configure the virtual server sections.

Click **Apply** at the bottom of the screen to save the above configuration.

QoS

QoS can let you classify Internet application traffic by source/destination IP address and port number. You can assign priority for each type of application and reserve bandwidth

for it. The packets of applications with higher priority will always go first. Lower priority applications will get bandwidth after higher priority applications get enough bandwidth. This can let you have a better experience in using critical real time services like Internet phone, video conference …etc. All the applications not specified by you are classified as rule name "Others". The rule with a smaller priority number has a higher priority; the rule with a larger priority number has a lower priority. You can adjust the priority of the rules by moving them up or down.

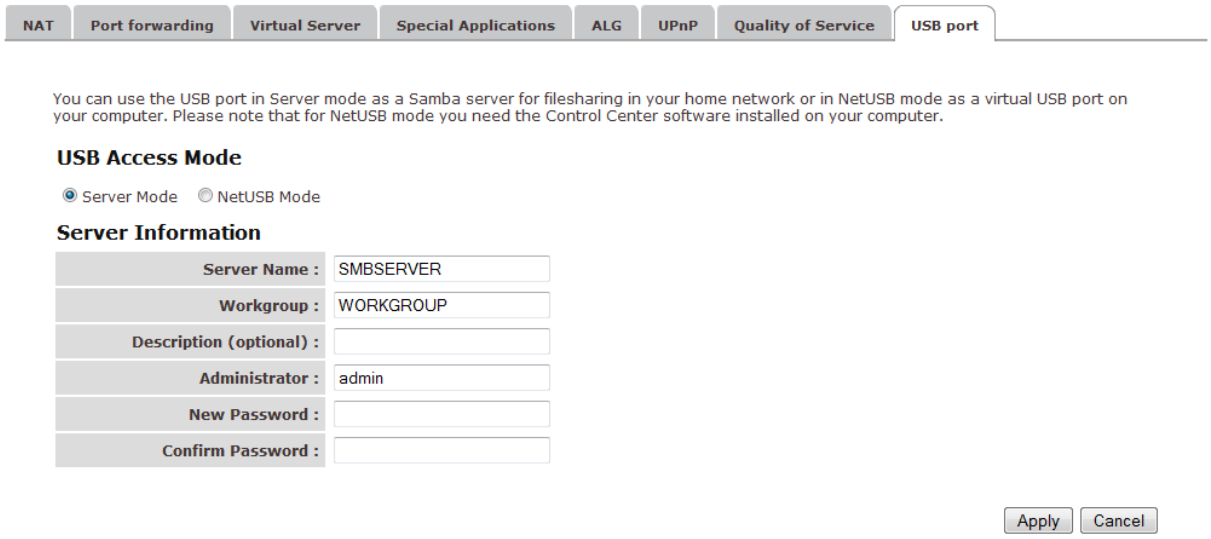

Wi-Fi Router X4 N300
SITECOM
Status | Internet Settings | 2.4GHz WiFi | Firewall | Advanced Settings | Toolbox
Choose your language
NAT | Port forwarding | Virtual Server | Special Applications | ALG | UPnP | Quality of Service
Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail.
QoS Enable
Current QoS Table :
Priority
Rule Name
Upload Bandwidth
Download Bandwidth
Select
Add
Edit
Delete Selected
Delete All
Move Up
Move Down
Reset
Apply
Cancel

- **Enable/Disable QoS**: You can check "Enable QoS" to enable QoS functionality for the WAN port.
- **Add a QoS rule into the table**: Click "Add" then enter a form of the QoS rule. Click "Apply" after filling out the form the rule will be added into the table.
- **Remove QoS rules from the table**: If you want to remove QoS rules from the table, select the QoS rules you want to remove in the table and then click "Delete Selected". If you want remove all QoS rules from the table, just click the "Delete All" button. Clicking "Reset" will clear your current selections.
- **Edit a QoS rule**: Select the rule you want to edit and click "Edit", then enter the detail form of the QoS rule. Click "Apply" after editing the form and the rule will be saved.
- **Adjust QoS rule priority**: You can select the rule and click "Move Up" to make its priority higher. You also can select the rule and click "Move Down" to make its priority lower.

Click **Apply** at the bottom of the screen to save the above configuration.

USB port

You can use the USB port in Server mode as a Samba server for filesharing in your home network or in NetUSB mode as a virtual USB port on your computer. Please note that for NetUSB mode you need the USB Port Control Center software installed on your computer.



- **Server name**: Enter a name for the network share.
- **Workgroup**: If you wish to add the share to your workgroup enter the workgroup name here.
- **Description**: Enter a desired description for the share.
- **Administrator**: Enter a desired username for access to the share.
- **New Password**: Enter the password for access to the share and confirm this password by re-entering it in the Confirm password field

For netUSB make sure the radio button next to netUSB is selected and press **Apply**. Please see Addendum A: USB Port Control Center for more information about netUSB.

Toolbox Settings

Sitecom Cloud Security

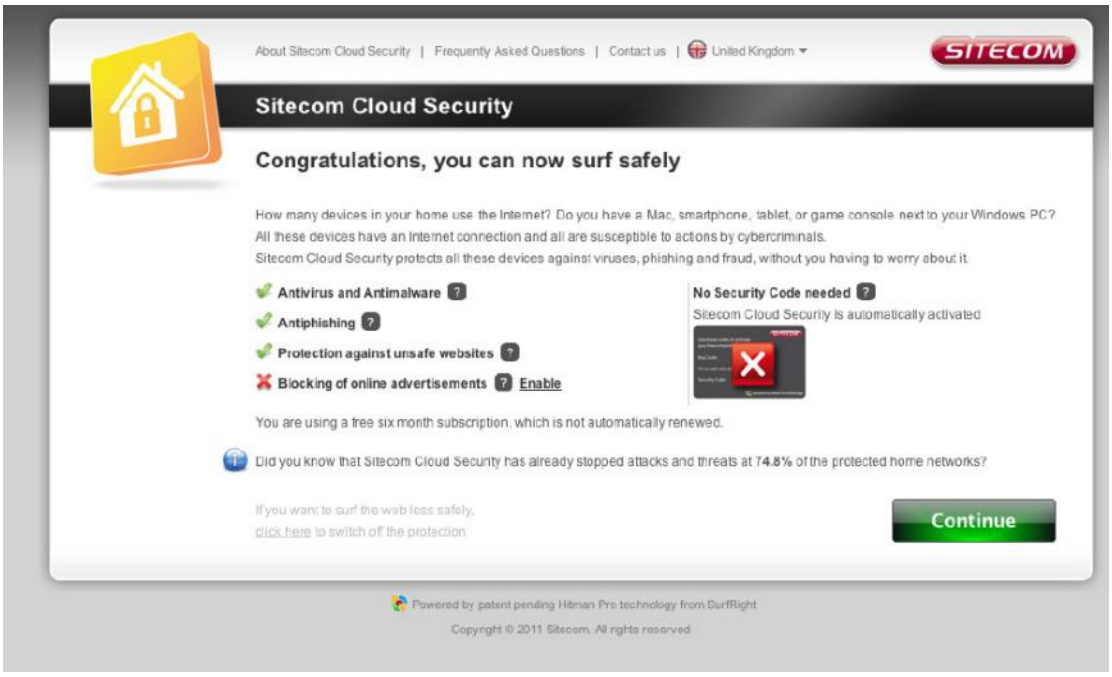
Antivirus software alone is not safe enough. You can now benefit from additional built-in security in your modem or router. Protect all devices in your home network against cybercrime while browsing. Activate in just one click, your network and devices are better secured than ever before.

Your Sitecom device comes with a 6 month free Sitecom cloud security subscription.

Activating Sitecom Cloud Security

After you have set up your Sitecom device for internet access, open the web browser and enter http://www.sitecomcloudsecurity.com in the address bar.

If the device has been properly configured the following web page should be shown.

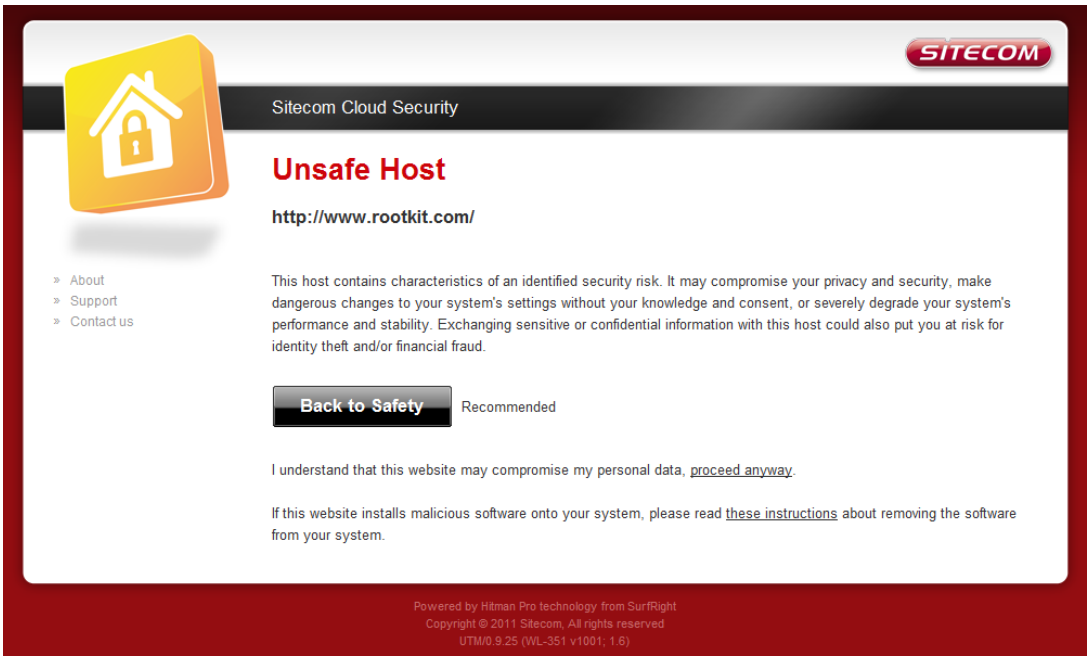

About Sitecom Cloud Security | Frequently Asked Questions | Contact us | United Kingdom
SITECOM
Sitecom Cloud Security
Congratulations, you can now surf safely
How many devices in your home use the Internet? Do you have a Mac, smartphone, tablet, or game console next to your Windows PC?
All these devices have an Internet connection and all are susceptible to actions by cybercriminals.
Sitecom Cloud Security protects all these devices against viruses, phishing and fraud, without you having to worry about it.
Antivirus and Antimalware
Antiphishing
Protection against unsafe websites
Blocking of online advertisements
Enable
No Security Code needed
Sitecom Cloud Security is automatically activated
You are using a free six month subscription, which is not automatically renewed.
Did you know that Sitecom Cloud Security has already stopped attacks and threats at 74.8% of the protected home networks?
If you want to surf the web less safely,
click here to switch off the protection
Continue
Powered by patent pending Hitman Pro technology from SurfRight
Copyright © 2011 Sitecom. All rights reserved

Here you can see which security features are activated.

The Sitecom Cloud Security service offers the following protection options:

- Anti-Malware
- Anti-Phishing
- Protection against unsafe websites
- Advertisement blocking

With the protection of unsafe websites activated the Sitecom Cloud Security will always check if a website is safe. If it is not safe it will inform you that is not safe to enter.

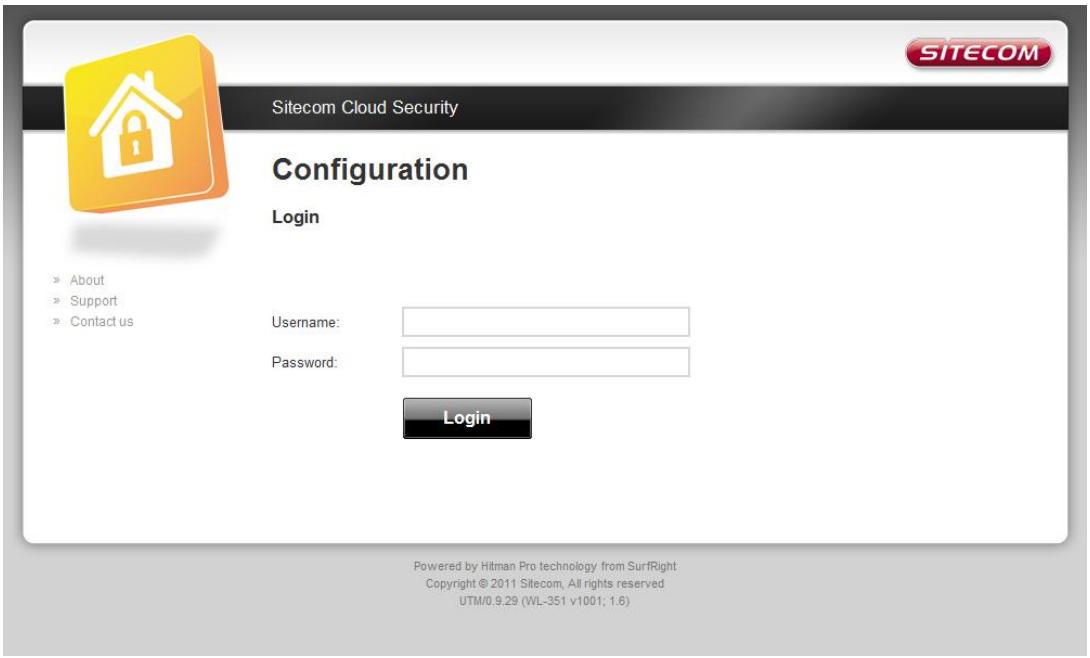

SITECOM
Sitecom Cloud Security
Unsafe Host
http://www.rootkit.com/
» About
» Support
» Contact us
This host contains characteristics of an identified security risk. It may compromise your privacy and security, make dangerous changes to your system's settings without your knowledge and consent, or severely degrade your system's performance and stability. Exchanging sensitive or confidential information with this host could also put you at risk for identity theft and/or financial fraud.
Back to Safety
Recommended
I understand that this website may compromise my personal data, proceed anyway.
If this website installs malicious software onto your system, please read these instructions about removing the software from your system.
Powered by Hitman Pro technology from SurfRight
Copyright © 2011 Sitecom, All rights reserved
UTM/0.9.25 (WL-351 v1001; 1.6)

If you still wish to visit this webpage click on 'proceed anyway'. Alternatively click 'Back to Safety' so that your security will not be breached.

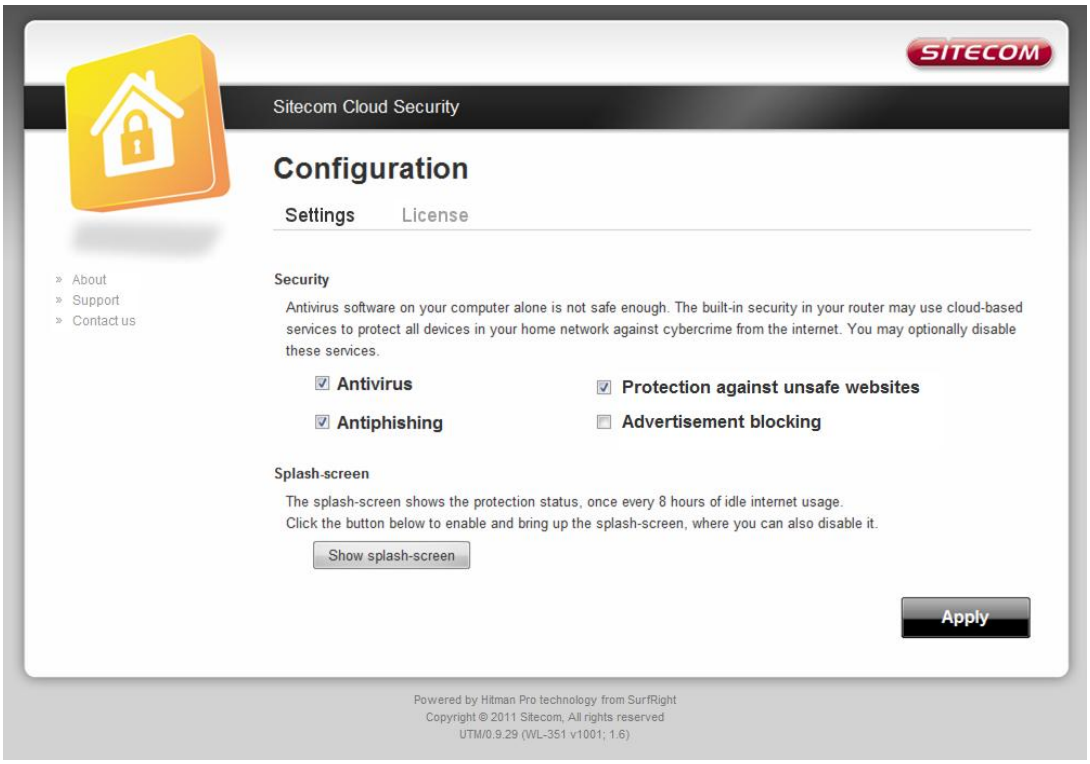
Configuring Sitecom Cloud Security

If you wish to change your security options or to extend your subscription at any time, open http://www.sitecomcloudsecurity.com from your web browser.

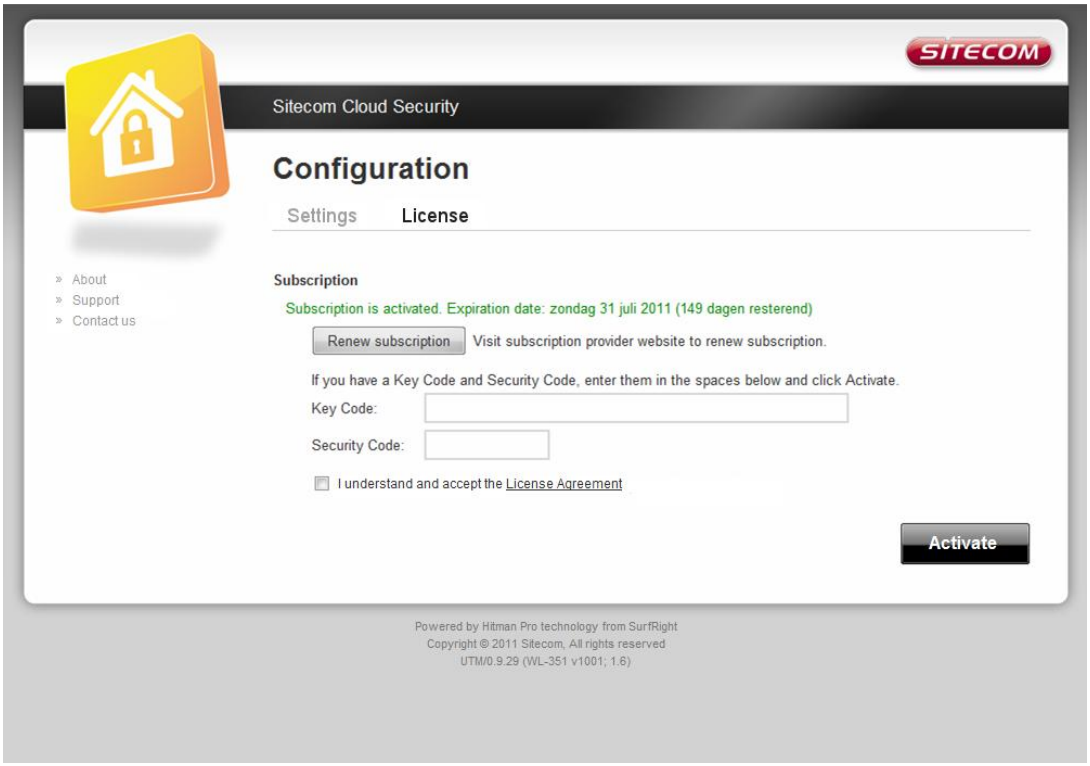
You will be asked for a username and password. These can be found on the backlabel on the bottom of your Sitecom router or modem.



If the login succeeded you can click on 'Settings' to change your security options.


SITECOM
Sitecom Cloud Security
Configuration
Settings
License
» About
» Support
» Contact us
Security
Antivirus software on your computer alone is not safe enough. The built-in security in your router may use cloud-based services to protect all devices in your home network against cybercrime from the internet. You may optionally disable these services.
Antivirus
Protection against unsafe websites
Antiphishing
Advertisement blocking
Splash-screen
The splash-screen shows the protection status, once every 8 hours of idle internet usage.
Click the button below to enable and bring up the splash-screen, where you can also disable it.
Show splash-screen
Apply
Powered by Hitman Pro technology from SurfRight
Copyright © 2011 Sitecom, All rights reserved
UTM/0.9.29 (WL-351 v1001; 1.6)

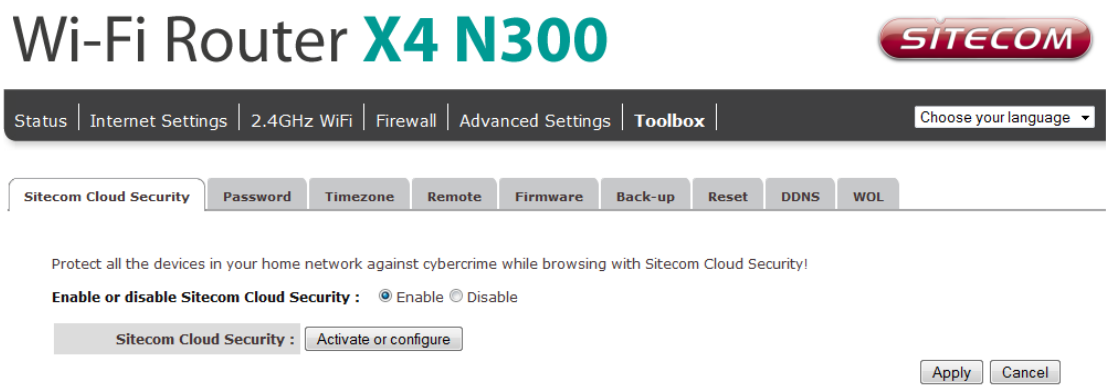
Or click 'License' to renew your subscription.


SITECOM
Sitecom Cloud Security
Configuration
Settings
License
» About
» Support
» Contact us
Subscription
Subscription is activated. Expiration date: zondag 31 juli 2011 (149 dagen resterend)
Renew subscription
Visit subscription provider website to renew subscription.
If you have a Key Code and Security Code, enter them in the spaces below and click Activate.
Key Code:
Security Code:
I understand and accept the License Agreement
Activate
Powered by Hitman Pro technology from SurfRight
Copyright © 2011 Sitecom, All rights reserved
UTM/0.9.29 (WL-351 v1001; 1.6)

Disabling Sitecom Cloud Security

If you wish to disable to Sitecom cloud security at any time, open the webpage of your Sitecom product and log in with the supplied credentials (these can be found on the back label on the bottom of your Sitecom device).

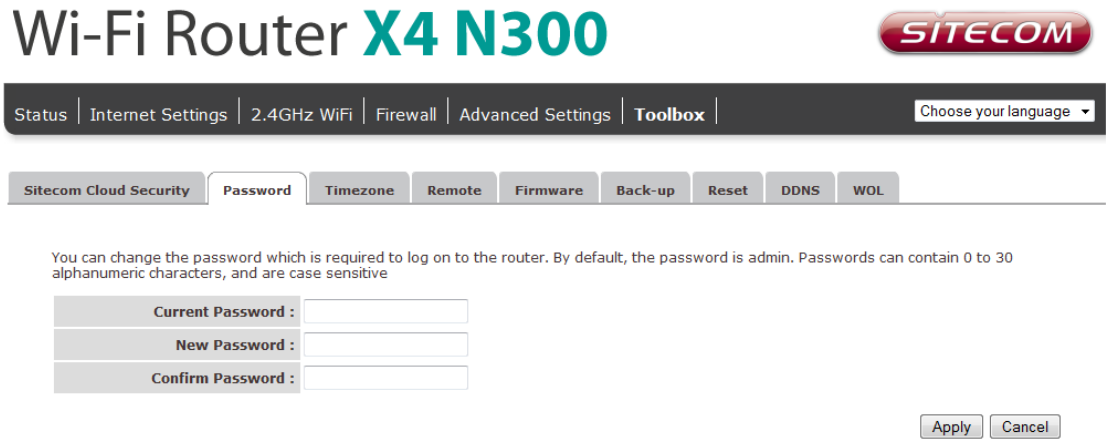
Go to Toolbox and select “Sitecom Cloud Security”.


Wi-Fi Router X4 N300
SITECOM
Status | Internet Settings | 2.4GHz WiFi | Firewall | Advanced Settings | Toolbox
Choose your language
Sitecom Cloud Security | Password | Timezone | Remote | Firmware | Back-up | Reset | DDNS | WOL
Protect all the devices in your home network against cybercrime while browsing with Sitecom Cloud Security!
Enable or disable Sitecom Cloud Security : Enable Disable
Sitecom Cloud Security : Activate or configure
Apply Cancel

Click the “Disable” radio button and click ‘**Apply’** for the settings to take effect.

Password

You can change the password required to log into the router's system web-based management. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.

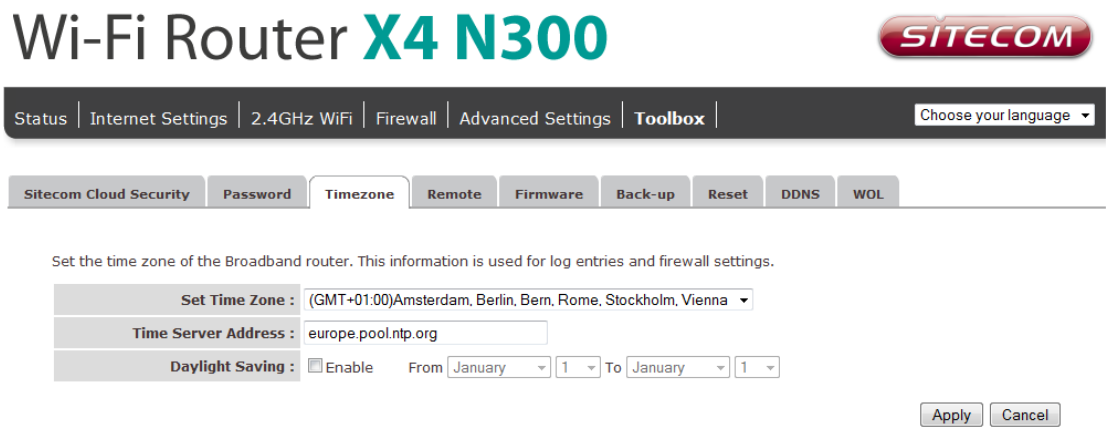

Wi-Fi Router X4 N300
SITECOM
Status | Internet Settings | 2.4GHz WiFi | Firewall | Advanced Settings | Toolbox
Choose your language
Sitecom Cloud Security | Password | Timezone | Remote | Firmware | Back-up | Reset | DDNS | WOL
You can change the password which is required to log on to the router. By default, the password is admin. Passwords can contain 0 to 30 alphanumeric characters, and are case sensitive
Current Password :
New Password :
Confirm Password :
Apply Cancel

- **Current Password**: Fill in the current password to allow changing to a new password.
- **New Password**: Enter your new password.
- **Confirmed Password**: Enter your new password again for verification purposes.

Click **Apply** at the bottom of the screen to save the above configuration.

Time Zone

The Time Zone allows your router to base its time on the settings configured here, which will affect functions such as Log entries and Firewall settings.

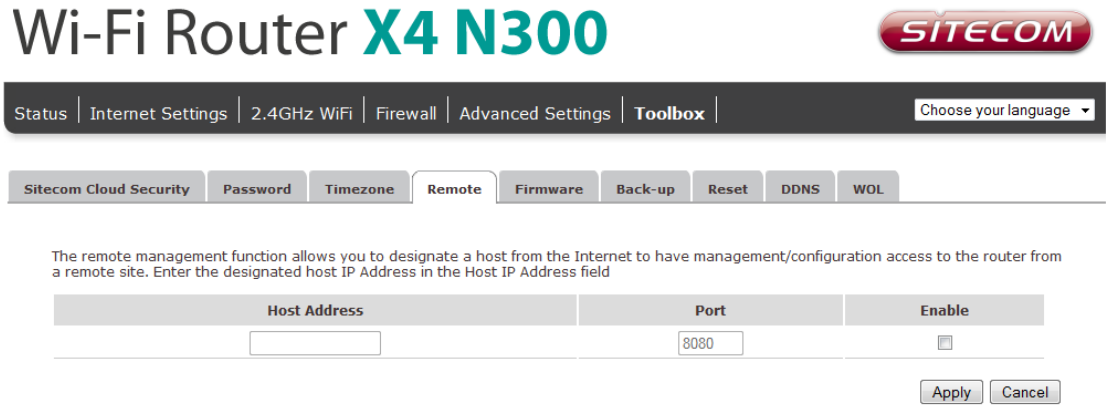

Wi-Fi Router X4 N300
SITECOM
Status | Internet Settings | 2.4GHz WiFi | Firewall | Advanced Settings | Toolbox
Choose your language
Sitecom Cloud Security | Password | Timezone | Remote | Firmware | Back-up | Reset | DDNS | WOL
Set the time zone of the Broadband router. This information is used for log entries and firewall settings.
Set Time Zone : (GMT+01:00)Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Time Server Address : europe.pool.ntp.org
Daylight Saving : Enable From January 1 To January 1
Apply Cancel

- **Set Time Zone**: Select the time zone of the country you are currently in. The router will set its time based on your selection.
- **Time Server Address:** You can set an NTP server address.
- **Enable Daylight Savings**: The router can also take Daylight savings into account. If you wish to use this function, you must check/tick the enable boxto enable your daylight saving configuration (below).
- **Start Daylight Savings Time**: Select the period in which you wish to start daylight Savings Time.
- **End Daylight Savings Time**: Select the period in which you wish to end daylight Savings Time.

Click **Apply** at the bottom of the screen to save the above configuration.

Remote Management

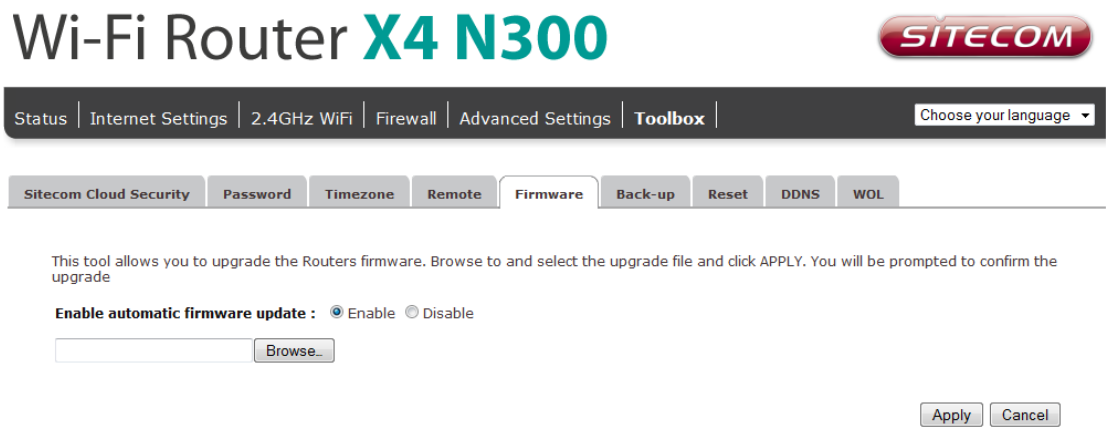
The remote management function allows you to designate a host in the Internet the ability to configure the Broadband router from a remote site. Enter the designated host IP Address in the Host IP Address field.


Wi-Fi Router X4 N300
SITECOM
Status | Internet Settings | 2.4GHz WiFi | Firewall | Advanced Settings | Toolbox
Choose your language
Sitecom Cloud Security | Password | Timezone | Remote | Firmware | Back-up | Reset | DDNS | WOL
The remote management function allows you to designate a host from the Internet to have management/configuration access to the router from a remote site. Enter the designated host IP Address in the Host IP Address field
Host Address
Port
Enable
8080
Apply Cancel

- **Host Address**: This is the IP address of the host in the Internet that will have management/configuration access to the Broadband router from a remote site. If the Host Address is left 0.0.0.0 this means anyone can access the router's web-based configuration from a remote location, providing they know the password.
- **Port**: The port number of the remote management web interface.
- **Enabled**: Select "Enabled" to enable the remote management function.

Click **Apply** at the bottom of the screen to save the above configuration.

Firmware Upgrade


Wi-Fi Router X4 N300
SITECOM
Status | Internet Settings | 2.4GHz WiFi | Firewall | Advanced Settings | Toolbox
Choose your language
Sitecom Cloud Security | Password | Timezone | Remote | Firmware | Back-up | Reset | DDNS | WOL
This tool allows you to upgrade the Routers firmware. Browse to and select the upgrade file and click APPLY. You will be prompted to confirm the upgrade
Enable automatic firmware update : Enable Disable
Browse...
Apply
Cancel

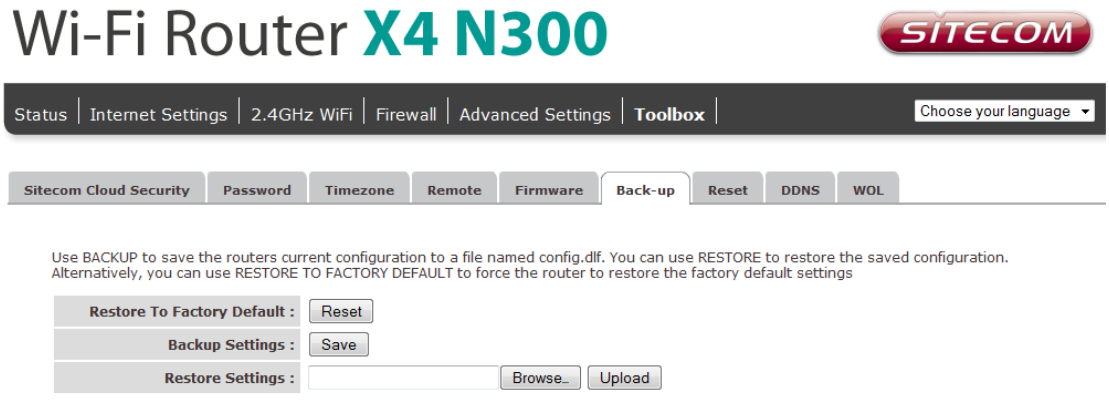
Enable automatic firmware update: When enabled the router will periodically check if a new firmware is available. If a new firmware is detected the router will give a notification.

Firmware Upgrade: This tool allows you to upgrade the Broadband router's system firmware. To upgrade the firmware of your Broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the Browse button to find the firmware file on your PC.

Once you've selected the new firmware file, click **Apply** at the bottom of the screen to start the upgrade process.

Backup Settings

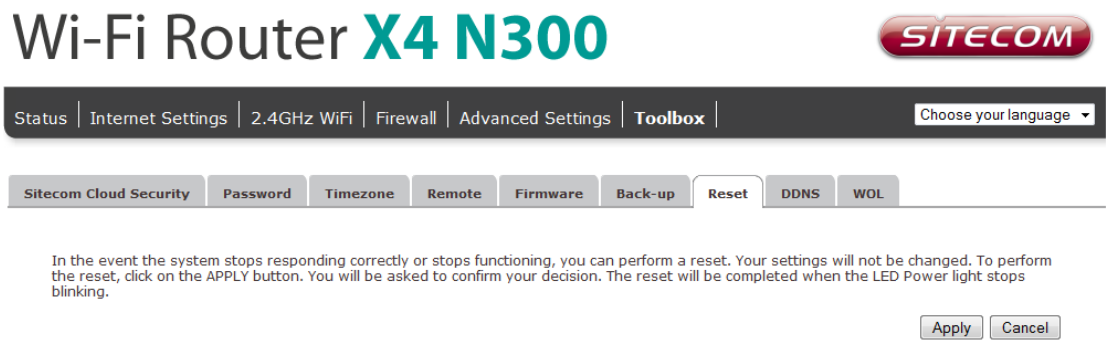
The Backup screen allows you to save (Backup) the current configuration settings. When you save the configuration setting (Backup) you can re-load the saved configuration into the router through the Restore selection. If extreme problems occur you can use the Restore to Factory Defaults selection, this will set all configurations to its original default settings (e.g. when you first purchased the router).


Wi-Fi Router X4 N300
SITECOM
Status | Internet Settings | 2.4GHz WiFi | Firewall | Advanced Settings | Toolbox
Choose your language
Sitecom Cloud Security | Password | Timezone | Remote | Firmware | Back-up | Reset | DDNS | WOL
Use BACKUP to save the routers current configuration to a file named config.dlf. You can use RESTORE to restore the saved configuration.
Alternatively, you can use RESTORE TO FACTORY DEFAULT to force the router to restore the factory default settings
Restore To Factory Default : Reset
Backup Settings : Save
Restore Settings : Browse... Upload

Use the "Backup" tool to save the current configuration to a file named "config.bin" on your PC. You can then use the "Restore" tool to restore the saved configuration to the router. Alternatively, you can use the "Restore to Factory Defaults" tool to force the router to perform a power reset and restore the original factory settings.

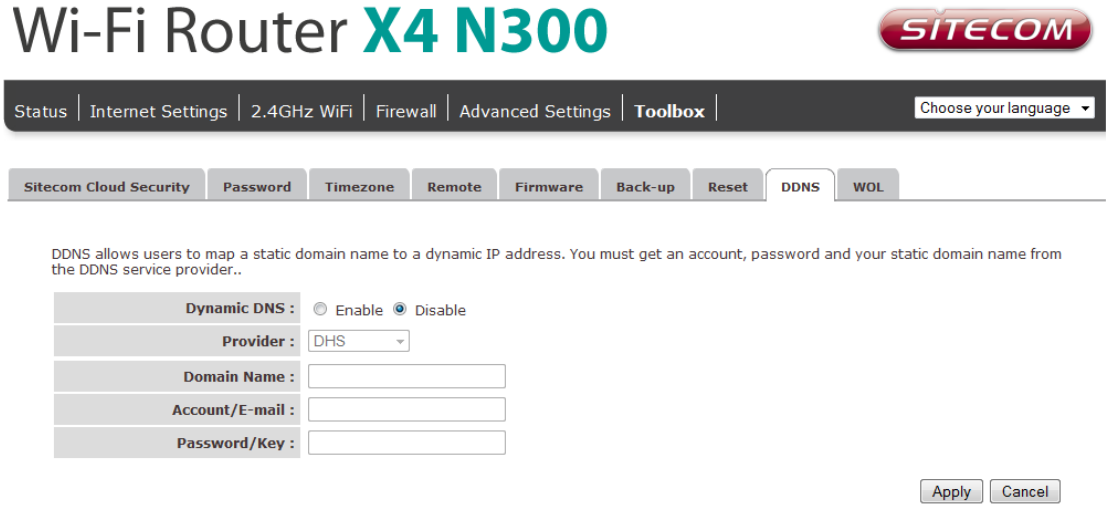
Reset

You can reset the router's system should any problem exist. The reset function essentially re-boots your router's system.



DDNS

DDNS allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers. This router supports DynDNS, TZO and other common DDNS service providers.



- **Enable/Disable**: Enable or disable the DDNS function of this router
- **Provider**: Select a DDNS service provider
- **Domain name**: Fill in your static domain name that uses DDNS
- **Account/E-mail**: The account that your DDNS service provider assigned to you
- **Password/Key**: The password you set for the DDNS service account above

Click **Apply** at the bottom of the screen to save the above configuration.

Addendum A: GNU/GPL Leaflet

Licensing Information

Parts of the firmware of the WLR-4100 WiFi Router X4 N300 are subject to the GNU general public license.

This product includes third-party software licensed under the terms of the GNU General Public License.. You can modify or redistribute this free software under the terms of the GNU General Public License. Please see Appendix B for the exact terms and conditions of this license.

Specifically, the following part of this product is subject to the GNU GPL:

#	Package name	Source
1	Linux v2.6.36	www.kernel.org
2	busybox v1.13	http://www.busybox.net/
3	uboot v1.1.3	http://www.denx.de/wiki/U-Boot
4	gcc v4.3.4	http://gcc.gnu.org/
5	iptables v1.4.4	http://www.netfilter.org/projects/iptables/index.html
6	iproute2-2.6.34	http://www.netfilter.org/projects/iptables/index.html
7	mtd-utils	http://processors.wiki.ti.com/index.php/MTD_Utilities
8	zlib v1.2.3	http://www.zlib.net/
9	termcap v1.3.1	ftp://ftp.gnu.org/gnu/termcap
10	pcre v6.x	http://www.pcre.org/
11	popt v1.7	http://freecode.com/projects/popt
12	libupnp v1.6.0	http://pupnp.sourceforge.net/
13	openssl-0.9.7	http://www.openssl.org/
14	flex-2.5.x	http://flex.sourceforge.net/
15	uclibc v0.9.29	http://www.uclibc.org
16	sqlite-3.7.x	http://www.sqlite.org/
17	udhcp v0.9.9-pre	http://sources.busybox.net/index.py/trunk/udhcp-web/index.html?revision=9967
18	igmpproxy v0.1-beta2	http://sourceforge.net/projects/igmpproxy
19	accel-pptp	http://sourceforge.net/projects/accel-pptp
20	brctl2	http://www.busybox.net/
21	utelnetd-0.1.9	http://sourceforge.net/projects/utelnetd

22	dnsmasq-2.x	http://thekelleys.org.uk/dnsmasq/doc.html
23	ppp v2.4.3	http://ppp.samba.org
24	rp-pppoe-3.x	http://www.roaringpenguin.com/products/pppoe
25	pptp-client	http://pptpclient.sourceforge.net/
26	linuxigd-1.x	http://www.sourceforge.net/projects/upnp
27	uuidgen	http://www.ossp.org/pkg/lib/uuid/
28	ez-ipupdate	http://sourceforge.net/projects/ez-ipupdate
29	updatedd-2.6	http://sourceforge.net/projects/updatedd
30	ntpclient	http://doolittle.icarus.com/ntpclient/
31	hotplug2-1.x	http://code.google.com/p/hotplug2/
32	udns-0.2.x	http://www.corpit.ru/mjt/udns.html#download
33	dnsmasq-2.5x	http://www.thekelleys.org.uk/dnsmasq/
34	wide-dhcpv6	http://sourceforge.net/projects/wide-dhcpv6/
35	ulogd-1.24	http://www.gnumonks.org/projects/ulogd
36	wget-1.11.x	http://www.gnu.org/software/wget/
37	ez-ipupdate	http://www.ez-ip.net.

Availability of source code

Sitecom Europe BV has made available the full source code of the GPL licensed software, including any scripts to control the compilation and installation of the object code on the Sitecom website.

No Warranty

The free software included in this product is distributed in the hope that it will be useful, but WITHOUT ANY LIABILITY OF OR ANY WARRANTY FROM THE LICENSOR.

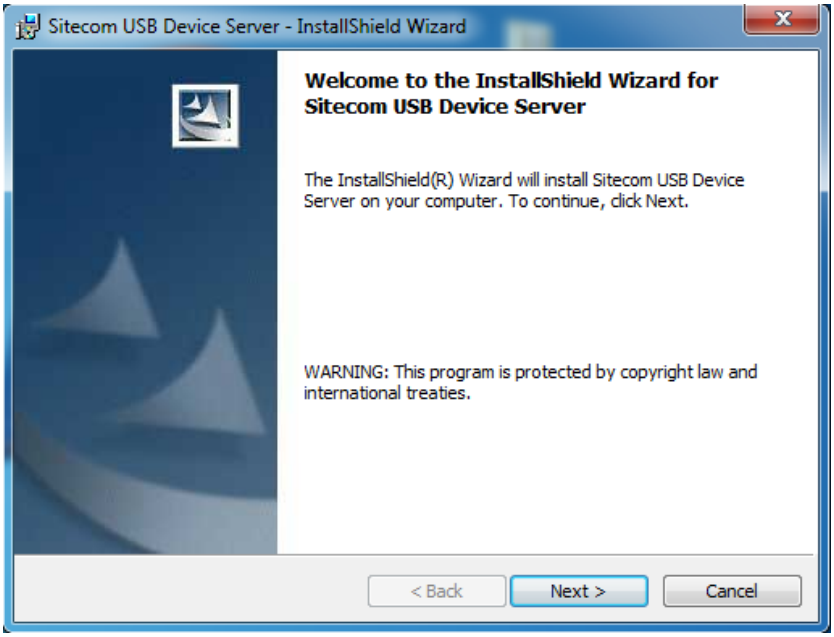
Addendum A: USB Port Control Center

The netUSB functionality of your router requires additional software to work with your computer. The following section will describe how the software can be installed and used.

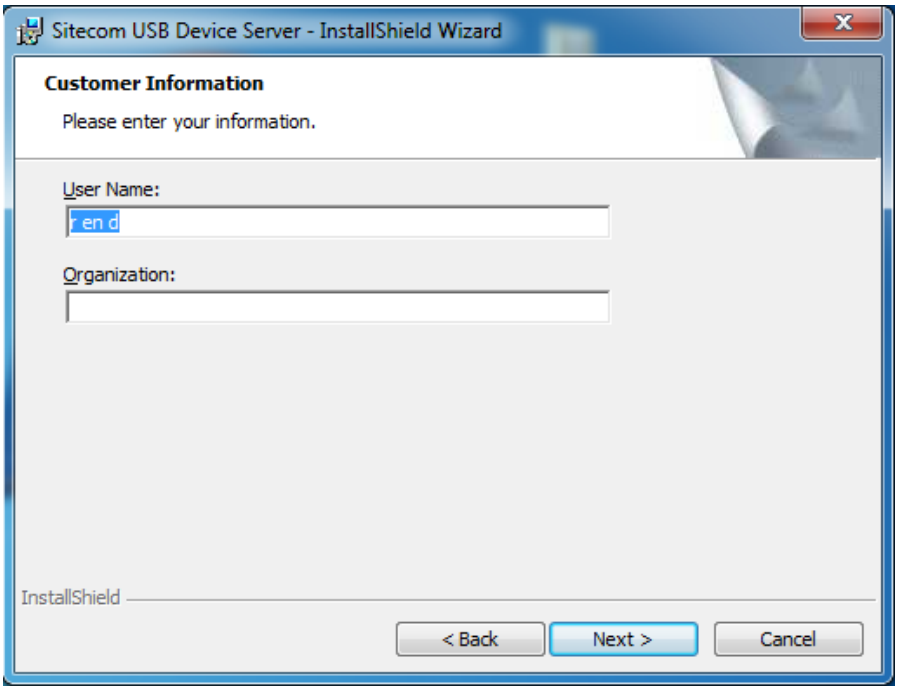
Windows

Insert the CD-ROM that was included with your router and select install utility from the cd-menu.

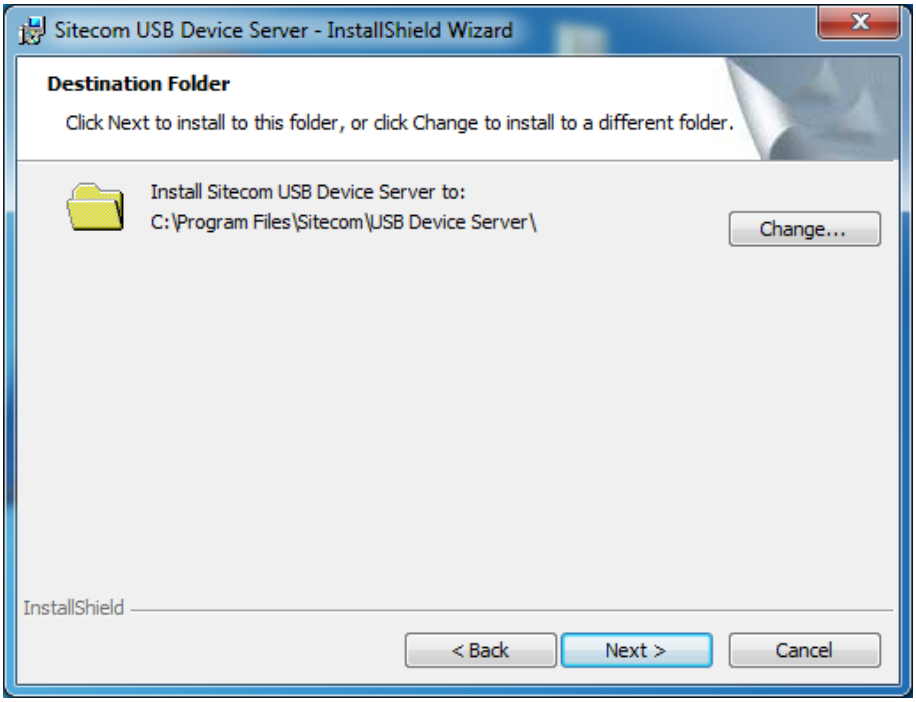
The software will inform you about what will be installed.


Sitecom USB Device Server - InstallShield Wizard
Welcome to the InstallShield Wizard for Sitecom USB Device Server
The InstallShield(R) Wizard will install Sitecom USB Device Server on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

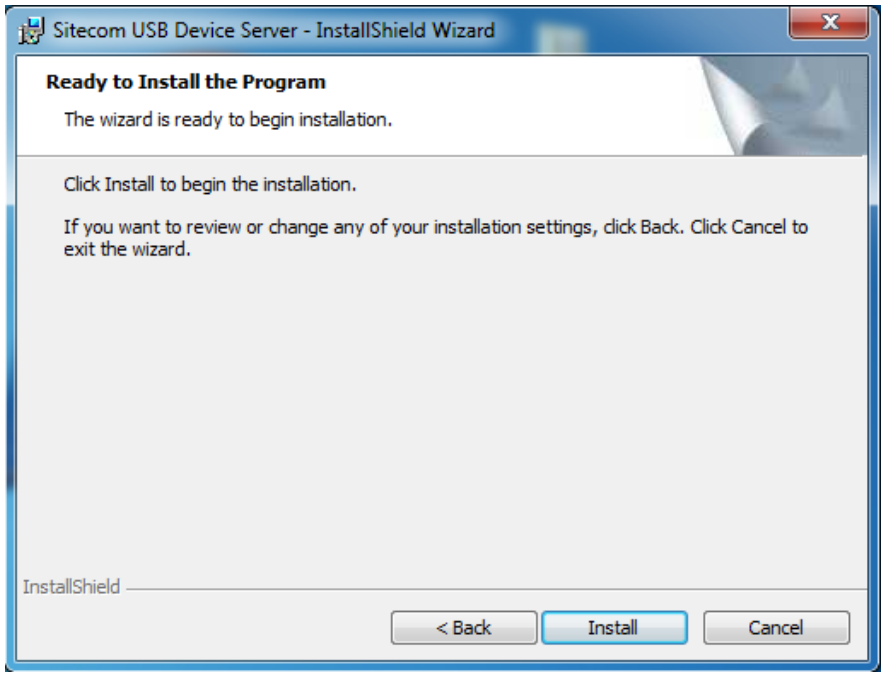
Click **Next** to continue the installation.



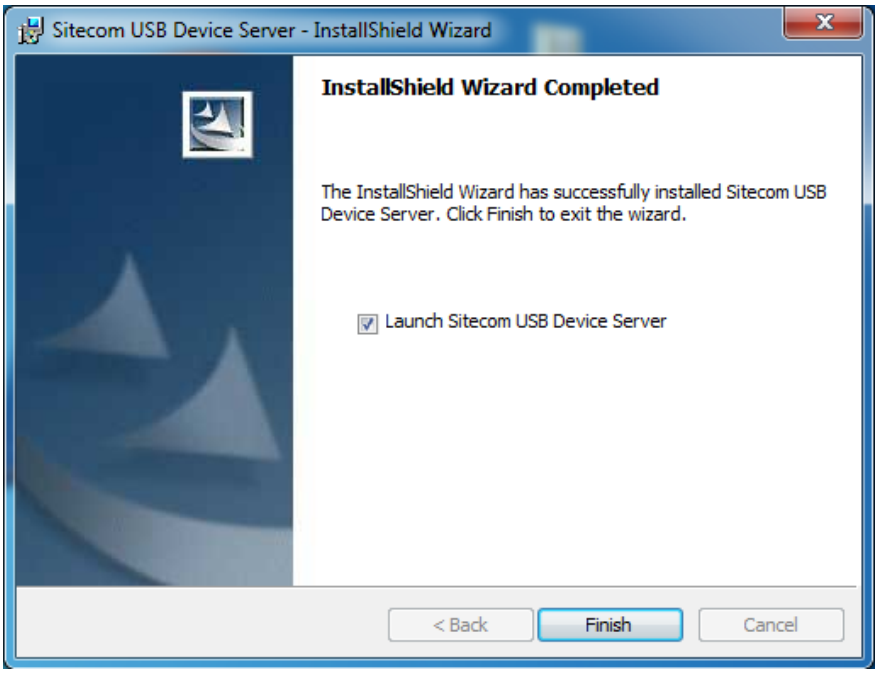
Enter your username and organization if applicable and click **Next** to continue.


Sitecom USB Device Server - InstallShield Wizard
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
Install Sitecom USB Device Server to:
C:\Program Files\Sitecom\USB Device Server\
Change...
InstallShield
< Back
Next >
Cancel

Choose a folder where the software should be installed or keep it to default and click **Next** to continue.


Sitecom USB Device Server - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

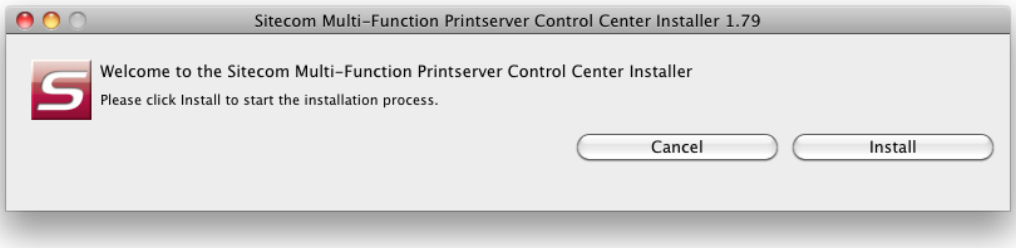
The software is now ready to be installed, Click **Install** to continue.


Sitecom USB Device Server - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed Sitecom USB Device Server. Click Finish to exit the wizard.
Launch Sitecom USB Device Server
< Back
Finish
Cancel

Once the installation is finished the software will inform you. If "**Launch Sitecom USB Device Server**" checked the software will automatically be launched after you clicked **Finish**.

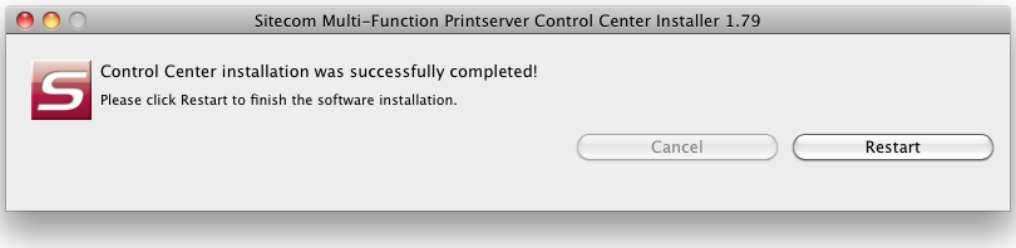
MacOS

Insert the CD-ROM that was included with your router and select "**Install**" from the cd-menu.


Sitecom Multi-Function Printserver Control Center Installer 1.79
Welcome to the Sitecom Multi-Function Printserver Control Center Installer
Please click Install to start the installation process.
Cancel
Install

Click **Install** to continue installation.

Enter your Mac username and password and click **OK** to continue.


Sitecom Multi-Function Printserver Control Center Installer 1.79
Control Center installation was successfully completed!
Please click Restart to finish the software installation.
Cancel
Restart

Once the installation is finished the software will inform you and requires to restart the system.

Connect & Disconnect

"NetUSB" allows you to use USB printers when they're actually connected to the Sitecom USB server.

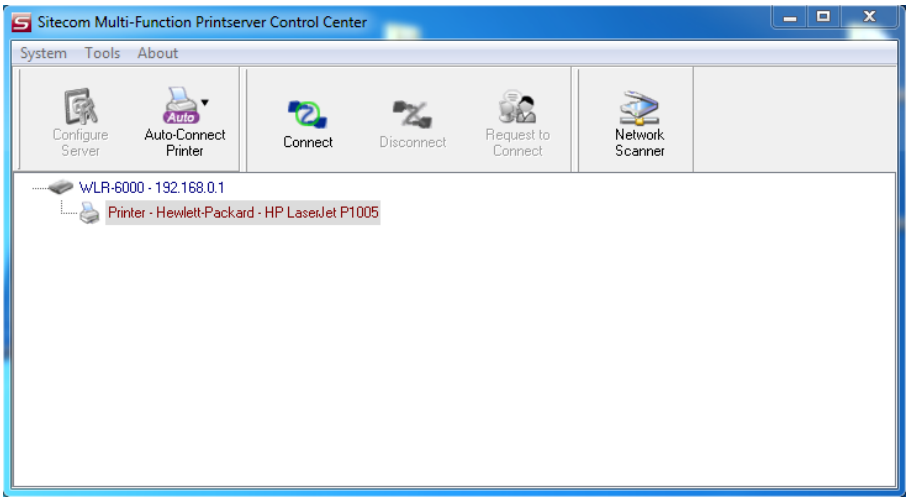
The "connect" operation is a software operation that simulates an actual USB device plug-in. Therefore, when you do a "connect" operation in the Control Center, the PC can detect a USB device's plug-in, although actually you do not plug in any USB device to your PC. Similarly, the "disconnect" operation is a software operation that simulates the disconnection of the USB device.

Note: If a USB device is "connected" by a PC, we say that PC has the ownership of the USB device. Only one PC can get the ownership of a USB device at the same time.

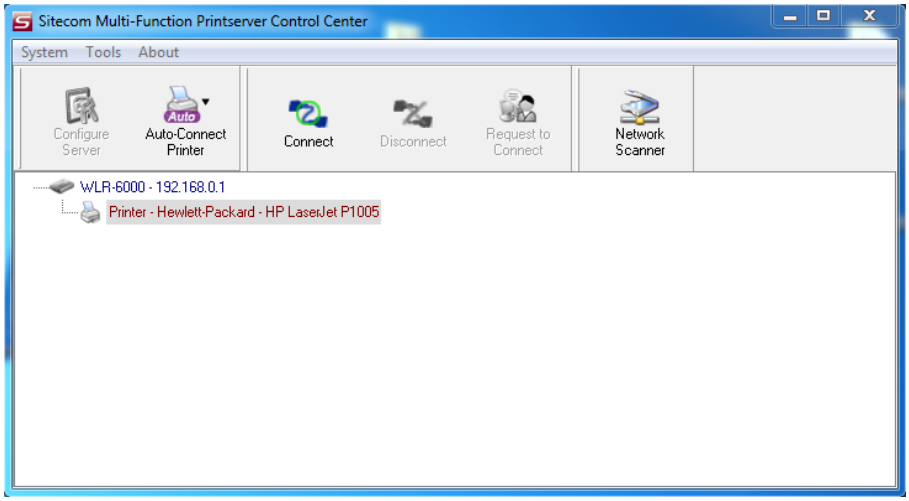
NetUSB installation

The steps to do installation for USB devices, like MFPs:

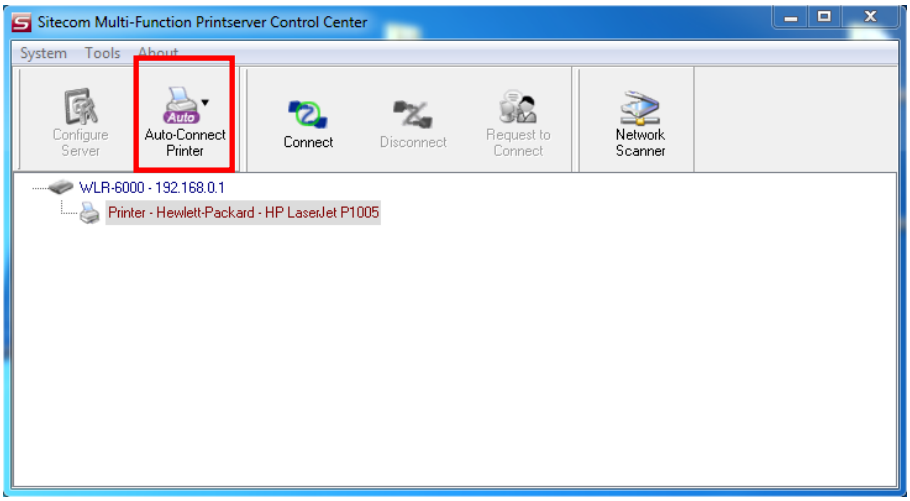
- Make sure the router is turned on.
- Connect the USB device to the USB port of the router.
- Run the Control Center. In the "USB MFP Server List" window, you can see the host names and IP addresses all of the Sitecom servers (in blue) on the network, as shown below.



- Click the server. Then all USB devices attached to the server will be shown.



- Please follow the user manual of the USB device to install its driver. For example, you may put the driver CD of the USB device in the CD-ROM player to install the driver.
- When you are asked to plug in the USB device into PC's USB port, click the desired USB device in the Control Center and then click the "Auto-Connect Printer" button to do the connect operation and get the ownership of the USB device. The computer name of the device owner will be shown at the end of the device.



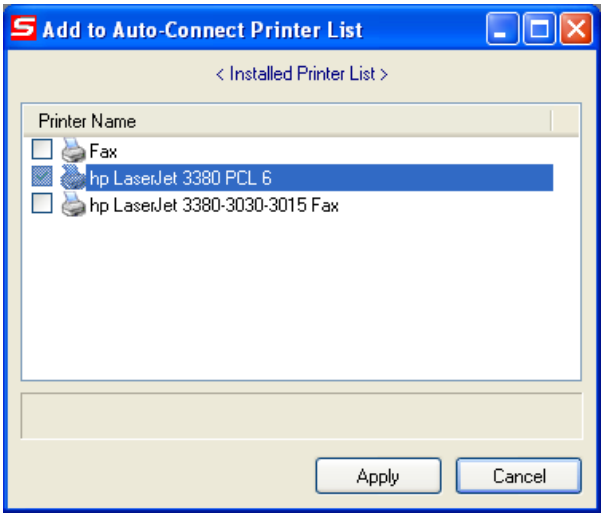
- PC will automatically detect that the USB device is plugged-in. On the right side of the Windows Task Bar, you can see the information of the new device. Continue to follow the user manual of the USB device to do the rest jobs of installation, until the driver installation has finished.

After the installation, you can see the newly created devices on the PC. If the USB device is a MFP, you can see a new printer and a new scanner from the "Control Panel".

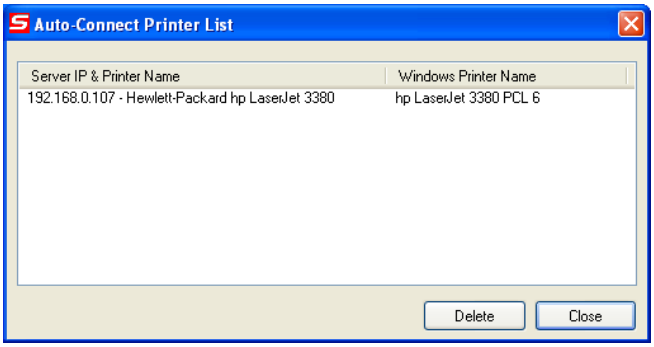
NetUSB Printing using Auto-Connect Printer

After the driver is installed, you can see a newly created printer in the Control Panel. Follow the steps below to perform NetUSB printing.

- In the Control Center, click the MFP server that has the desired printer (or MFP) attached.
- Click the desired printer (or MFP).
- Click the "Auto Connect Printer" button and choose "Set Auto-Connect Printer". The following figure will appear.



- Choose the desired printer. The desired printer must be the Windows printer (this is a logical printer) that matches the printer attached on the MFP server (this is a physical printer). Then click the "**Apply**" button.



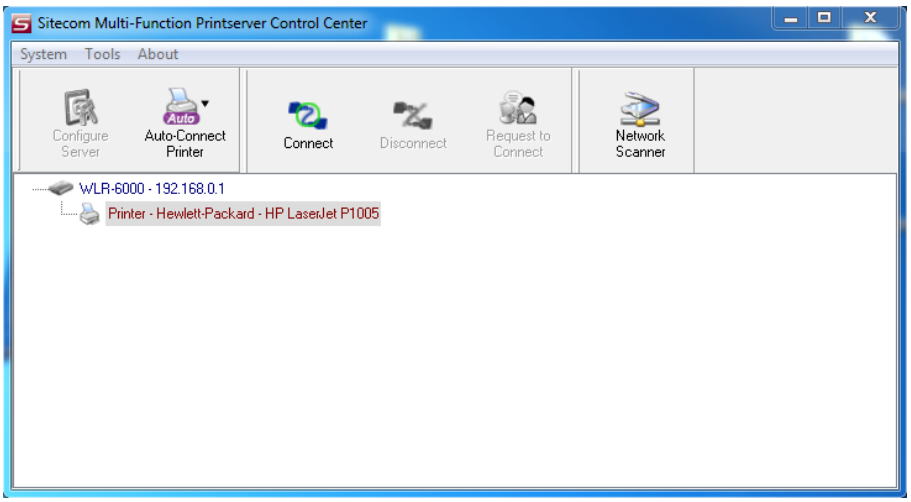
- Then, the printer will be marked as an "Auto-Connected Printer" in red. If you choose "Auto-Connected Printer List" in the "Tools" menu, you can see a newly created item that describes the association between the Windows printer and the physical printer on the server.
- Then try to issue a print job to the desired printer. You will see the Control Center will automatically do a connect operation and, once the print job finished, it will hold the connection. However, the connection will be released immediately when another user do the printing afterward. At the same time, the printer is automatically disconnected with your PC.

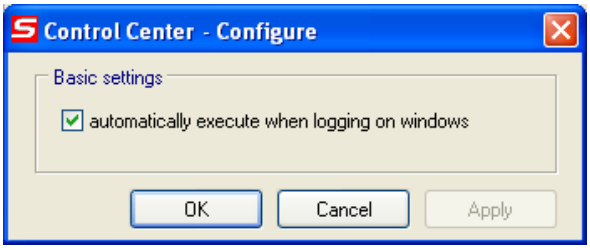
- When you do a print job again. The control center will automatically do a connecting operation on printing again. This is so-called "Auto Connect / Disconnect" operation.

Note: Under the "Auto-Connected Printer" setting, it is not necessary to manually press the "**Connect**" button when printing. If you press the "Connect" button for printing, please make sure to click "**Disconnect**" button after you finish the printing. Otherwise, other users cannot print properly. It is because you are the only ownership of the connected printer.

AutoRun

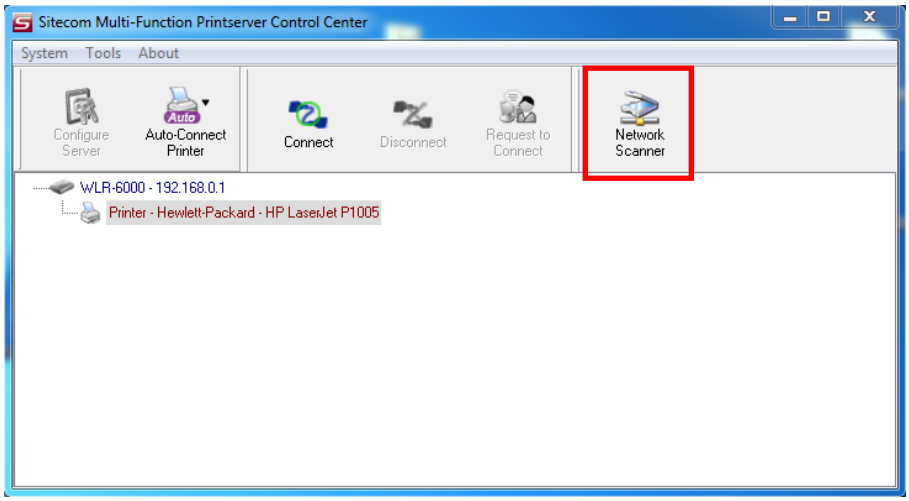
You can make the Control Center be run automatically after you login Windows. To do this, you choose the "Configuration" item in the "Tools" menu. The following window will appear. Click the check box and then on the "OK" button. This feature is enabled by default.



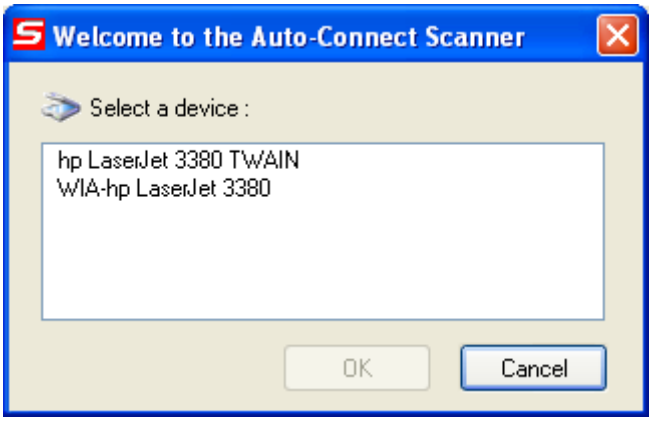


NetUSB Scanning using Network Scanning

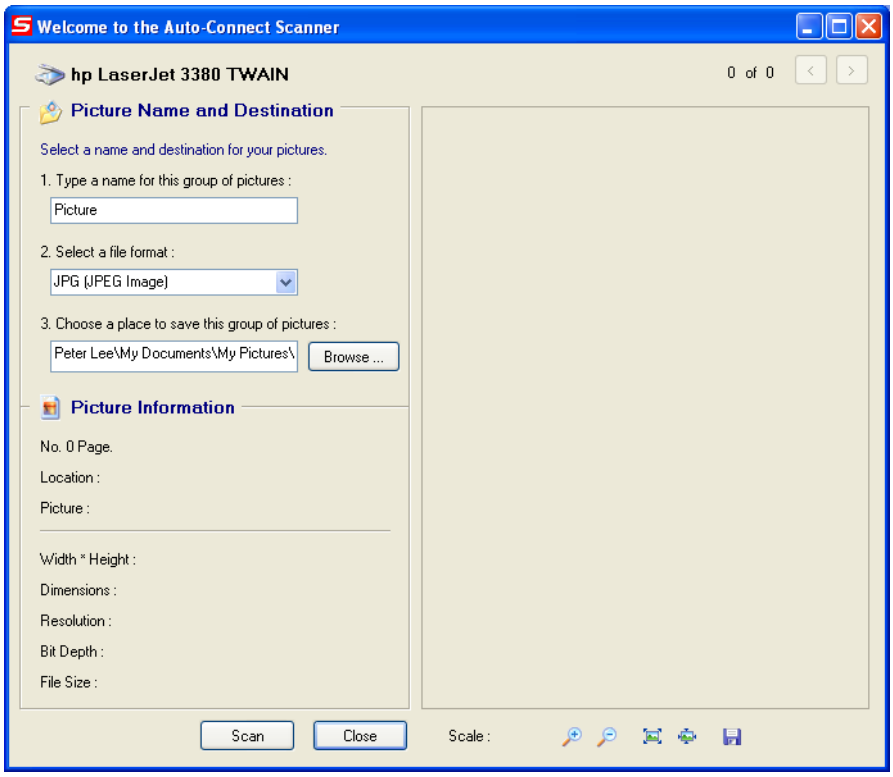
- In the Control Center, click the MFP server that has the desired MFP attached.
- Click the desired MFP.
- Click the "Network Scanner" button.



- Then you can see that the Control Center will automatically do a "connect" operation. The following window will appear.



- Choose one of TWAIN or WIA item. Click "OK". The following window will appear.



- Follow the usual steps to do scanning.

Addendum C: GNU/GPL

Version 3, 29 June 2007 Copyright © 2007 Free Software Foundation, Inc. http://fsf.org/

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

“This License” refers to version 3 of the GNU General Public License.

“Copyright” also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

“The Program” refers to any copyrightable work licensed under this License. Each licensee is addressed as “you”. “Licensees” and “recipients” may be individuals or organizations.

To “modify” a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a “modified version” of the earlier work or a work “based on” the earlier work.

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to “keep intact all notices”.

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual

works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A “User Product” is either (1) a “consumer product”, which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, “normally used” refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

“Installation Information” for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the

User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license,

and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's “contributor version”.

A contributor's “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the

patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is “discriminatory” if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

Addendum C: Declaration of Conformity

Sitecom Europe BV

EC Declaration of Conformity

We
Sitecom Europe BV
Linatebaan 101
3045 AH Rotterdam
The Netherlands

Hereby declare under our sole responsibility that the Sitecom product:

Product number:	WLR-4100 v1 001
Product description:	Wi-Fi Router N300 X4

To which this declaration relates is in conformity with the requirements of the following standards:

CE/LVD
- EN 60950-1: 2006+A11 (2009)

CE/EMC
- EN 301 489-1 V1.8.1
- EN 301 489-17 V2.1.1

RADIO SPECTRUM
- EN 300 328 V1.7.1 2006-10
- EN 50385 2002

This certifies that the following designated Sitecom product:

Product description: Wi-Fi Router N300 X4
Product No.: WLR-4100 v1 001

Complies with the requirements of the following directives and carries the CE marking accordingly:
R&TTE Directive 99/5/EC, EMC directive 2004/95/EC and Low Voltage Directive 2006/95/EC.
This declaration is the responsibility of the manufacturer / importer:

Sitecom Europe B.V.
Rotterdam, 10 August 2012

P. Schoonenberg,

CEO

UK CE COMPLIANCE

Hereby Sitecom Europe BV declares that this product is in accordance with essential requirements and other relevant terms of the European regulation 1999/5/EC.

FR CONFORMITE CE

Par la présente Sitecom Europe BV, déclare que l'appareil est conforme aux exigences essentielles et aux dispositions pertinentes de la Directive Européenne 1999/5/EC.

DE CE-CONFORMITÄT

Hiermit erklärt Sitecom Europe BV, dass dieses Produkt die erforderlichen Voraussetzungen und andere relevante Konditionen der europäischen Richtlinie 1999/5/EC erfüllt.

IT CONFORMITA ALLE NORME CE

Con la presente Sitecom Europe BV dichiara che questo prodotto è conforme ai requisiti essenziali e agli altri termini rilevanti della Direttiva Europea 1999/5/EC.

NL CE GOEDKEURING

Hierbij verklaart Sitecom Europe BV dat dit product in overeenstemming is met de essentiële eisen en andere relevante bepalingen van Europese Richtlijn 1999/5/EC.

ES CONFORMIDAD CON LA CE

Por la presente Sitecom Europe BV declara que este producto cumple con los requisitos esenciales y las otras provisiones relevantes de la Directiva Europea 1999/5/EC.

PT CONFORMIDADE CE

Pela presente a Sitecom Europe BV declara que este produto está em conformidade com os requisitos essenciais e outras condições relevantes da regulamentação Europeia 1999/5/EC.

SE CE-FÖRSÄKRAN

Härmed försäkrar Sitecom Europe BV att denna produkt uppfyller de nödvändiga kraven och andra relevanta villkor EU-direktivet 1999/5/EC.

DK OVERENSSTEMMELSESERKLÆRING

Sitecom Europe BV bekræfter hermed, at dette produkt er i overensstemmelse med væsentlige krav og andre betingelser i henhold til Rådets direktiv 1999/5/EC.

NO CE-OVERENSSTEMMELSE

Sitecom Europe BV erklærer herved at dette produktet er i overensstemmelse med de avgjørende kravene og andre relevante vilkår i den europeiske forskriften 1999/5/EC.

FI CE-HYVÄKSYNTÄ

Täten Sitecom Europe BV ilmoittaa, että tämä tuote on yhdenmukainen direktiivin 1999/5/EC olennaisten vaatimusten ja muiden asiaankuuluvien sopimusehtojen kanssa.

RU СООТВЕТСТВИЕ ТРЕБОВАНИЯМ CE

Настоящим компания Sitecom Europe BV заявляет, что ее продукция соответствует основным требованиям и условиям Европейской Директивы 1999/5/EC.

PL CERTYFIKAT ZGODNOŚCI CE

Sitecom Europe BV niniejszym oświadcza, że ten produkt spełnia wszelkie niezbędne wymogi, a także inne istotne warunki dyrektywy europejskiej 1999/5/WE.

GR ΣΥΜΜΟΡΦΩΣΗ ΜΕ CE

Η Sitecom Europe BV δηλώνει, διά του παρόντος, ότι αυτό το προϊόν συμμορφώνεται με τις ουσιώδεις απαιτήσεις και τους λοιπούς όρους του ευρωπαϊκού κανονισμού 1999/5/EC.

RoHS compliant

This product may be used in the following countries:

AT BE HU CZ IT RO EE ES
FI FR IS NL GR CY LI DE
LT LU LV MT GB SI TR PT
SE SK PL DK CH BG NO U

For non EU countries please check with the local authorities for restrictions of using wireless products